Gestão de Redes e Sistemas

Estudo de um caso

Jorge André Marques de Andrade

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Arquitetura, Sistemas e Redes

Orientador(a): Doutora Maria João Ferreira Viamonte

Júri:

Presidente:
Doutora Isabel de Fátima Silva Azevedo

Vogais:
Doutora Maria João Monteiro Ferreira Viamonte
Doutor Luís Miguel Moreira Lino Ferreira

Porto, Outubro de 2015

Resumo

A gestão e monitorização de redes é uma necessidade fundamental em qualquer organização, quer seja grande ou pequena. A sua importância tem de ser refletida na eficiência e no aumento de informação útil disponível, contribuindo para uma maior eficácia na realização das tarefas em ambientes tecnologicamente avançados, com elevadas necessidades de desempenho e disponibilidade dos recursos dessa tecnologia.

Para alcançar estes objetivos é fundamental possuir as ferramentas de gestão de redes adequadas. Nomeadamente ferramentas de monitorização. A classificação de tráfego também se revela fundamental para garantir a qualidade das comunicações e prevenir ataques indesejados aumentando assim a segurança nas comunicações. Paralelamente, principalmente em organizações grandes, é relevante a inventariação dos equipamentos utilizados numa rede.

Neste trabalho pretende-se implementar e colocar em funcionamento um sistema autónomo de monitorização, classificação de protocolos e realização de inventários. Todas estas ferramentas têm como objetivo apoiar os administradores e técnicos de sistemas informáticos.

Os estudos das aplicações que melhor se adequam à realidade da organização culminaram num acréscimo de conhecimento e aprendizagem que irão contribuir para um melhor desempenho da rede em que o principal beneficiário será o cidadão.

Palavras-chave: Gestão de Redes, Monitorização, Classificação de Tráfego, Desempenho.

Abstract

This project was designed to study solutions for managing networks and systems, based on the current growth and development of information technology. The constant evolution carries out new monitoring needs and finding the most adequate tools for decision support and management is crucial.

At the same time, the classification of traffic is a very important issue in several activities related to the networks, such as the prediction of QoS, security, monitoring, accounting, planning backbones capacity, and intrusion detection. The variation of certain types of traffic can influence technical decisions in the area of network management as well as political and social decisions.

In this work we intend to implement and operate an independent monitoring system, classification of protocols and conducting inventories. All these tools are intended to support administrators and technicians of computer systems.

The studies of the applications that best suit the reality of the organization resulted in an increase in knowledge and learning that will contribute to a better performance of the network in which the main beneficiary will be the citizen.

Keywords: Network Management, Monitoring, Traffic Classification, Performance

Agradecimentos

A realização deste trabalho só foi possível com o apoio e ajuda de várias pessoas às quais quero expressar a minha gratidão.

Agradecimento especial à Doutora Maria João Viamonte, foi minha professora da unidade curricular Configuração e Gestão de Sistemas. Foi ela que despertou em mim este desejo de quer saber mais sobre assuntos relacionados com a gestão de redes e segurança.
Durante o desenvolvimento deste trabalho mostrou-se muito disponível para esclarecer dúvidas e orientou-me dizendo quais os temas que deveria focar.

Agradeço ao Ex. Presidente da Câmara Municipal de Santo Tirso Doutor Joaquim Couto, sem o seu consentimento para a realização deste trabalho nunca o poderia ter feito.

Agradeço ao Sr. Carneiro, chefe de gabinete dos serviços de informática, e a todos os meus colegas de serviço que se mostraram sempre disponíveis para esclarecer qualquer dúvida.

Especiais agradecimentos os meus colegas de mestrado com quem colaborei na realização de trabalhos e atividades nas aulas. Principalmente aos meus colegas e amigos, Ricardo Lisboa e Hugo Brandão.

Por último, não posso esquecer a minha família. Agradeço do fundo do meu ser o apoio da minha mãe e também, ao meu pai que de certeza me apoiava se estivesse fisicamente ao meu lado.
Agradeço ao meu irmão Doutor António Andrade porque é ele que devo todo meu percurso académico realizado até ao dia de hoje. É por mim e também por ele que quero ser sempre bem-sucedido.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos

ACK - Acknowledgment

ARP - Address Resolution Protocol

ATM - Asynchronous Transfer Mode

CMIP - Common Management Information Protocol

CMIS - Common Management Information Service

CPU - Central Processing Unit

CRC - Cyclic Redundancy Check

DDoS - Distributed DoS

DHCP - Dynamic Host Configuration Protocol

DLC - Data Link Control

DNS - Domain Name Server

DoS - Denial of Service

FC - Fiber Chanel

FCAPS - Fault, Configuration, Accounting, Performance, Security

FDDI - Fiber Distributed Data Interface

FTP - File Transfer Protocol

GPL - General Public License

HTTP - HyperText Transfer Protocol

HTTPS - HyperText Transfer Protocol Secure

ICMP - Internet Control Message Protocol

IMAP - Internet Message Access Protocol

IP - Internet Protocol

IPsec - Internet Protocol Security

IPX - Internetwork Packet Exchange

ISO - International Organization for Standardization

IOS - Internetwork Operating System

ITU-T - International Telecommunications Union - Telecommunication Standardization Sector

LAN - Local Area Network

LDAP - Lightweight Directory Access Protocol

MAC - Media Access Control

MIB - Management Information Base

MRTG - Multi Router Grapher

MO - Management Object

NAT - Network Address Translation

NDO - Nagios Data Out

NEB - Nagios Event Broker

NFS- Network File System

NIDS - Network Intrusion Detection System

NMS - Network Management System

NNTP - Network News Transfer Protocol

NNTPS - Nntp Protocol over TLS SSL

NSCA - Nagios Service Check Acceptor

NX-OS - Network Operating System designed by Cisco Systems

OID - Object Identifier

OSI - Open System Interconnection

PBX - Private Branch Exchange

PDU - Protocol Data Unit

PEM - Privacy Enhanced Mail

PNG - Portable Network Graphics

POP - Post Office Protocol

QoS - Quality of service

RAM - Random Access Memory

RFC - Request for Comments

RMON - Remote Network Monitoring

RRD - Round Robin Database

S/MIME - Secure/Multipurpose Internet Mail Extensions

SCTP - Stream Control Transmission Protocol

SMTP - Send Mail Transfer Protocol

SNMP - Simple Network Management Protocol

SQL - Structured Query Language

SSH - Secure Shell

SSL - Secure Sockets Layer

SYN - Synchronize

TCP – Transmission Control Protocol

TLS - Transport Layer Security

TMN - Telecommunication Management Network

UDP - User Datagram Protocol

WAN - Wide Area Network

WEP - Wired Equivalent Privacy

1. Introdução

Vivemos na era tecnológica. Hoje em dia, a internet e os sistemas que nela operam são imprescindíveis nas infraestruturas de comunicação das empresas que desejam ser tecnologicamente avançadas.

No mundo globalizado, os empresários necessitam de se destacar tecnologicamente de forma a atingir níveis de produtividade superiores. Este avanço acarreta consigo alguns investimentos em equipamentos e em *software* para que seja mantida a qualidade de serviço (QoS) das aplicações e dos protocolos utilizados nas comunicações.

Este aumento de complexidade das redes exige necessariamente um sistema de gestão para proporcionar a qualidade de serviço possível e desejada.

Com a complexidade das redes e o aumento do número de *routers*, *switches* e servidores dificultaram a gestão de todos esses equipamentos. Por exemplo, a certeza que estou em funcionamento e com um ótimo desempenho. (Schmidt, 2005)

Nos próximos capítulos, o leitor terá a oportunidade de tomar conhecimento de um exemplo prático da implementação de um sistema de gestão e de monitorização de uma rede com os mais variados equipamentos e aplicações. Para esta monitorização e gestão será dado a conhecer as várias tecnologias envolvidas e configuração da infraestrutura.

Todo este trabalho de estudo e planeamento será posto em prática numa infraestrutura já em funcionamento mas sem um sistema de monitorização global. Será implementado e configurado para a rede da Câmara Municipal de Santo Tirso.

1.1 Enquadramento Temático

Nas duas últimas décadas verificou-se um aumento da utilização da internet, do uso de aplicações que utilizam esta infraestrutura como meio e mais recentemente a utilização de serviços na própria internet (*Cloud Computing*), conduzindo à necessidade de implementação de sistemas de monitorização.

Conduzindo à necessidade de se aumentar as larguras de banda para uma maior receção e transmissão de dados para o exterior das organizações e aumentar o nível de segurança das comunicações com a utilização de cifras.

A Gestão de Redes e Sistemas é essencial nas organizações devido ao aumento de utilizadores que utilizam a internet e intranet. É necessário controlar e analisar o tráfego de dados neste meio de comunicação porque a sua capacidade é finita. É necessário filtrar os dados e classificá-los de acordo com as necessidades dos utilizadores.

Também é necessário monitorizar os equipamentos que constituem a infraestrutura de comunicações da organização. Os sistemas de monitorização são essenciais para a verificação do estado dos equipamentos e caso haja alguma anomalia o administrador deve ser notificado para proceder de forma rápida e objetiva na resolução do problema.

A análise do tráfego consiste na verificação dos diferentes protocolos que são utilizados pelas aplicações e dar-lhes diferentes prioridades na utilização da largura de banda. Este processo faz com que a qualidade de serviço (QoS) aumente tal como a satisfação dos seus utilizadores.

1.2 Objetivos e Principais Contribuições

Com esta Dissertação é pretendido documentar um estudo/trabalho no âmbito da Gestão de Redes e Sistemas na Câmara Municipal de Santo Tirso.

Com a introdução dos Sistemas de Informação a utilização crescente de aplicações de rede para agilização de processos e o aumenta das infraestruturas com mais equipamentos fez com que seja fulcral a monitorização dessas aplicações, equipamentos e protocolos que são utilizados nas comunicações.

Com este trabalho pretende-se aumentar a qualidade de serviço, a segurança e a rapidez de deteção de anomalias na rede da Câmara Municipal de Santo Tirso, para que os técnicos e administradores da rede possam agir em conformidade para a resolução de problemas.

Todas estas tarefas terão de ser implementadas por um conjunto de ferramentas distintas, e podendo estas comunicar, ou não entre si. O seu principal objetivo é a realização de relatórios detalhados sobre o tráfego da rede e o envio de notificações de problemas que estejam a acontecer na rede.

Este trabalho apresenta um estudo detalho sobre as diferentes ferramentas de gestão e as suas principais características. Este sistema de monitorização foi implementado num ambiente muito rico, com várias aplicações de rede e vários equipamentos ativos de rede que necessitam de ser monitorizados constantemente.

1.3 Organização da Dissertação

Neste primeiro capítulo, Introdução, é efetuado o enquadramento do tema deste trabalho, Gestão de Sistemas e Redes, sendo também apontados os principais objetivos do trabalho, bem como as suas contribuições.

No segundo capítulo, Introdução à Gestão de Redes, são introduzidos os conceitos gerais sobre a gestão de redes, é discutida a sua importância, assim como qual a contribuição dada para apoiar as decisões de gestão, fundamentais para o bom funcionamento de uma infraestrutura de rede. São descritas as áreas funcionais, arquiteturas e os seus modelos de informação e comunicação.

No terceiro capítulo, Aplicações de Monitoração, é dado a conhecer algumas ferramentas disponíveis para apoiar a atividade de gestão de redes, assim como é feita uma análise comparativa das mesmas.

No quarto capítulo, Arquitetura de Rede e Serviços na Câmara Municipal de Santo Tirso, é dado a conhecer a infraestrutura da rede de dados nesta instituição assim como os serviços instalados nos servidores disponíveis.

No quinto capítulo, Sistema de Monitorização na Câmara Municipal de Santo Tirso, é apresentado o sistema de monitorização proposto, assim como as ferramentas elegidas.

No sexto capítulo, Conclusões, são apresentadas as conclusões, ideias para trabalho futuro e os objetivos cumpridos.

2. Introdução à Gestão de Redes

2.1.Introdução e Definições

Um dos principais fatores que levaram ao desenvolvimento do ser humano tal como o conhecemos hoje foi sem dúvida a sua capacidade de comunicar e fazer-se entender. Ao longo dos tempos esta capacidade de comunicar, enviar e receber mensagens foi-se desenvolvendo em várias formas e com o uso de diversas tecnologias.

O exemplo de Tony Bautts é muito simples mas de facto bastante elucidativo do que é uma rede.

"*The idea of networking is probably as old as telecommunications itself. Consider people living in the Stone Age, when drums may have been used to transmit messages between individuals.*
Suppose caveman A wants to invite caveman B over for a game of hurling rocks at each other, but they live too far apart for B to hear A banging his drum. What are A's options? He could

1) walk over to B's place,

2) get a bigger drum, or

3) ask C, who lives halfway between them, to forward the message. The last option is called networking" (Tony Bautts, 2005)

Através da citação anterior verifica-se que os equipamentos intermédios são essenciais numa rede estruturada de dados, são eles que encaminham as mensagens para os recetores.
Estes equipamentos têm de ser constantemente monitorizados em tempo real porque caso haja alguma falha toda a infraestrutura de comunicação de dados fica comprometida. Isto trás enormes inconvenientes e, por vezes, prejuízos no negócio das organizações.

Pode-se então definir *networking* como uma tecnologia de comunicação em rede, onde só faz sentido quando existe elementos que transmitem as mensagens do emissor até ao recetor sem haver perda de informação. Estes elementos intermédios são chamados de equipamentos ativos de rede.

As ferramentas de gestão e monitorização dos equipamentos ativos de rede e de sistemas têm a tarefa fundamental de verificar os seus estados de uma forma periódica. Estas ferramentas recolhem informações e analisam-nas segundo um conjunto de regras. Entre essas informações, encontram-se

quais os protocolos que estão ser utilizados, que computadores ocupam mais largura de banda, que equipamentos e sistemas deixaram de responder, entre outras.

De uma forma prática, após o administrador de rede ser notificado devido a uma anomalia é-lhe apresentado um conjunto de dados importantes e desta forma pode atuar na sua resolução de uma forma rápida e objetiva.

Caso não exista uma ferramenta de monitorização a tarefa da resolução de uma anomalia pode levar horas ou mesmo dias, dependendo do tamanho da rede e do número de equipamentos. Torna-se uma tarefa desgastante porque poderá ser necessário verificar cada um dos equipamentos para descobrir em qual deles está o problema.

Qual a posição dos administradores de rede numa organização?

Segundo o documento desenvolvido por (Alexander Clemm, 2006)

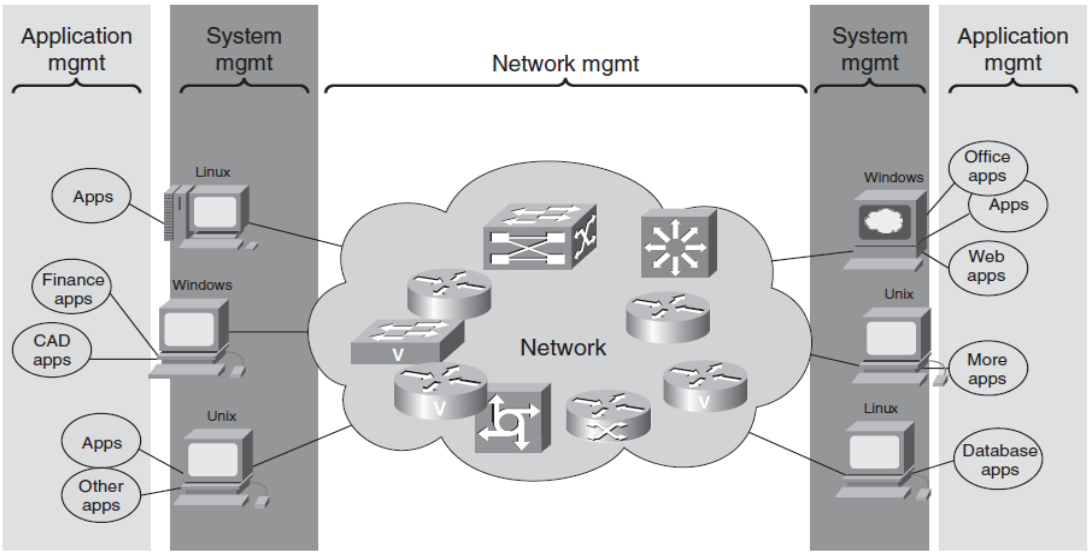


Figura 1 – Monitorização de Redes, Sistemas e aplicações. (Alexander Clemm, 2006)

Esta figura demonstra que para se administrar uma rede é necessário efetuar a monitorização de três grandes grupos:

- A rede como uma infraestrutura;
- Os sistemas que nela operam e;
- As aplicações que usam essa infraestrutura.

2.2.Importância da Gestão de Redes

Existe uma correlação entre negócio, redes e a sua gestão porque numa organização tecnologicamente avançada necessita de ter um conjunto de aplicações/serviços em ótimo estado de funcionamento para que o negócio da empresa não seja comprometido. Serviços tais como DHCP, DNS, Fileserver, sql Server etc.

Os serviços de IT *(Information Technology*) têm a função de monitorizar estes serviços de forma a que os colaboradores da empresa possam ter as condições necessárias para elaborarem as suas funções na organização, sem comprometer o seu negócio e a sua produtividade. Na maioria dos casos a indisponibilidade destes ou outros serviços traduz-se na perda em dinheiro para a organização.

É natural ocorrerem falhas, tais como humanas, ou dos próprios equipamentos, mas é exigido aos colaboradores de IT que minimizem ou, caso seja possível, eliminem as ocorrências dessas falhas.
Para se poder atingir este objetivo os administradores de redes têm de possuir um conjunto de conhecimentos e dispor da ajuda de sistemas de monitorização, contribuindo para que essas falhas sejam detetadas atempadamente ou as correções dessas falhas sejam automatizadas.

Para esta tarefa, por vezes, é necessário o investimento em equipamento e em recursos humanos devidamente qualificados para implementarem e assegurarem o seu bom funcionamento.

Depois das considerações feitas anteriormente verifica-se a importância da gestão de redes para o negócio das organizações. De uma forma prática, caso haja uma falha de um equipamento, ou de uma aplicação, é necessário que os administradores da rede sejam notificados para seja possível a resolução do problema com prejuízo mínimo para os utilizadores.

«Dada a criticidade que os sistemas de informação representam para o sucesso das organizações há necessidade de [os CIO] terem uma visibilidade, em tempo real, do que está a acontecer, designadamente nas diferentes componentes dos SI – redes, sistemas, base de dados, aplicações, transações, utilizadores e segurança (lógica e física)» – , afirma **Sérgio Sá***, security practice* diretor de *Global Managed Services da* ***Unisys***. (SérgioSá, 2012)

No testemunho anterior pode-se verificar que num contexto prático a monitorização dos equipamentos ativos de rede são de facto fundamentais para garantir o bom funcionamento do sistema.

Na área da segurança das comunicações também é essencial monitorizar os dados que circulam na rede. Nos dias de hoje um simples ataque de DoS (*Denial of service*) pode comprometer todas as comunicações e causar prejuízos na área de negócio das empresas.

«Na área de segurança, na qual a *AnubisNetworks* atua, temos visto uma preocupação crescente em monitorizar este tipo de eventos, pois um simples ataque pode prejudicar bastante a reputação e a marca de uma empresa» (Francisco Fonseca, 2012)

Penso que é de elevada importância que as empresas se preocupem em perceber a importância na monitorização dos equipamentos ativos de rede e quais são os prejuízos reais em caso de falha destes equipamentos, não esquecendo de contabilizarem o tempo e dinheiro que se pode perder para resolver um problema quando não existe monitorização.
Por vezes as empresas só conhecem a importância da monitorização e segurança quando algo acontece e prejudica gravemente o negócio das empresas.

«As empresas devem fazer uma análise *top down* desde os processos de negócio até aos elementos de TI que o suportam, e perceber o seu impacto na cadeia global, compreendendo assim o que tem de ser monitorizado de forma prioritária e sabendo como o monitorizar.» (José Ferraz, 2012)

Como podemos ver no testemunho anterior a qualidade e o nível do conhecimento das equipas de administradores de redes tem um enorme impacto no funcionamento dos vários sistemas de comunicação dentro de uma empresa e são um elemento fulcral e centralizador de uma organização.

2.3.Modelos de Gestão de Redes

Para melhor definir o âmbito de gestão de redes foram criados vários modelos de gestão. Os modelos de gestão de redes servem para organizar as diferentes tarefas e funcionalidades. Com os modelos é mais fácil executar a monitorização dos sistemas ou as operações de suporte na infraestrutura.

Alguns modelos de gestão estão amplamente estabelecidos e documentados.

O modelo OSI (*Open Systems Interconnection*) define cinco áreas funcionais ao qual vulgarmente se dá o acrónimo de FCAPS (*Fault*, *Configuration*, *Accounting*, *Performance* e *Security*).

Gestão de Falhas	Gestão de Configuração	Gestão de Contabilização	Gestão de Performance	Gestão de Segurança
Deteção de Falha Correção Isolamento	Iniciação do Recurso	Monitorização de utilização de um serviço – Cotas de utilização	Utilização de recurso e monitoração desse recurso	Gestão e monitorização de ameaças
Teste de Diagnostico	Rede e configuração de serviços	Monitorização de cotas pelos utilizadores	Satisfação na utilização do recurso pelos utilizadores	Gestão e certificação dos acessos dos utilizadores
Monitorização de rede	Configuração de políticas de gestão e automação	Gerar relatórios de cotas utilizadas	Análise de dados e planeamento de capacidade	Garantia de Segurança
Log de erros	Gestão de utilizadores – Registo e suporte	*Logs* e estatística	*Logs* e estatística	*Logs*, análise de dados e estatística
Correlações	*Logs* e estatística			

2.3.1. Gestão de falhas

A gestão de falhas trata das falhas que ocorrem na rede, nos equipamentos, nas aplicações e também nas comunicações. É uma gestão focalizada na monitorização da rede e que assegura o seu bom funcionamento e que gera notificações quando existe algum problema. Logo é um tipo de gestão muito importante porque garante a disponibilidade do meio a todos os utilizadores.

A deteção de falhas envolve 4 etapas: Primeiro é necessário detetar a falha ou ser notificado que existe uma falha. De seguida analisar os dados recolhidos sobre a falha e tentar determinar a sua origem e o porquê de a mesma ter acontecido. Após esta análise pode-se elaborar um diagnóstico e a proceder à correção da falha.

O objetivo principal é detetar e resolver rapidamente o problema que colocou em causa o bom funcionamento da rede ou do recurso.

2.3.2. Gestão de configuração

A gestão de configuração tem como principal função a monitorização das condições da rede, isto é identificar as mudanças de estado dos dispositivos monitorizados assim como a colocação de novos equipamentos.

Aquando da colocação e instalação de novos equipamentos na rede infraestruturada é fundamental informar o sistema de monitorização destes novos equipamentos.
É necessário configurar as suas políticas de gestão, atualizar o *firmware* dos equipamentos para garantir a sua melhor performance.
Garantir a conexão física e lógica dos equipamentos assim como o registo e suporte dos utilizadores.

2.3.3. Gestão de contabilização

A gestão de contabilização confere uma monitorização dos custos e tarifas dos equipamentos que são monitorizados. Sendo assim, pode-se contabilizar o uso dos recursos da rede numa organização. Por exemplo a largura de banda utilizada para o envio e receção e *emails*, VOIP etc. Todos estes dados utilizados nestes recursos devem ser contabilizados para que os administradores de rede tenham a real perceção dos gastos dos recursos da rede.

2.3.4. Gestão de performance

A gestão de desempenho é uma forma de medir, monitorizar e avaliar os níveis de desempenho da rede. Assegurar uma boa capacidade de tráfego da rede para não comprometer os recursos necessários ao negócio da organização.

2.3.5. Gestão de segurança

A gestão de segurança define um conjunto de políticas que garantam a boa utilização da rede na organização e minimizar a utilização abusiva da mesma.

Além disto deve assegurar a segurança do próprio sistema de gestão não permitindo o acesso a funções essenciais e de controlo da rede. Assim como garantir a confidencialidade e integridade dos dados.

Os direitos de acesso aos meios e aos recursos devem ser personalizados aos diferentes agentes e utilizadores da rede para garantir um elevado grau de segurança. Esta personalização é configurada através de políticas de segurança

2.4.Arquiteturas de Gestão de Redes

Numa gestão de redes existem dois elementos essenciais: o gestor propriamente dito e o objeto a ser gerido. O gestor de rede é um dispositivo com características ao nível do *hardware* e *software* capaz de intercetar informação e processá-la. Existem várias aplicações/serviços capazes de realizar estas tarefas, sendo algumas pagas outras gratuitas.

O objeto gerido é algo que deve ser gerido e verificado de uma forma periódica. Por exemplo, monitorização de espaço num disco rígido, memórias ou mesmo o estado de um *link* entre dispositivos.

Para ser possível a realização destas tarefas é necessário que o objeto gerido contenha algum tipo de "Base de Dados" com dados disponíveis de ser consultados pelo gestor. Estas "Bases de Dados" são chamadas de MIB's (*Management information base*). Para que o gestor consiga consultar as MIB's terá de utilizar um protocolo de comunicação, O SNMP (*Simple Network Management Protocol*). (Cisco, 2012)

2.4.1. Arquitetura centralizada

Este tipo de arquitetura é a mais comum nos vários modelos de gestão.

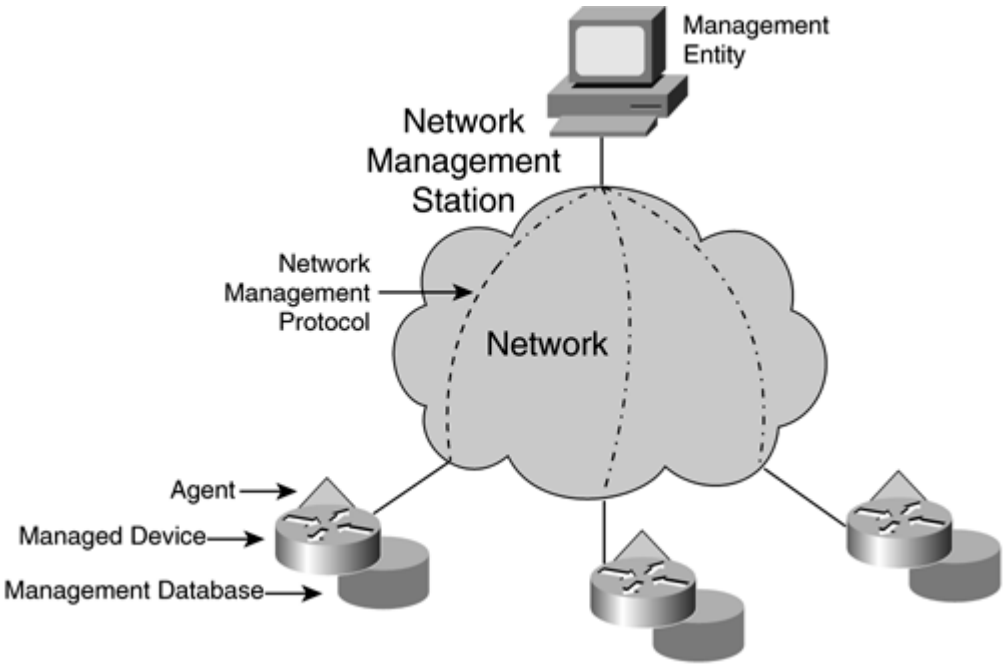


Figura 2 - Gestão Centralizada (Castelli, 2002)

Pode-se verificar através da figura anterior que numa gestão centralizada os objetos geridos (*"Managed Device"*) têm de conter uma MIB.

O gestor (*"Management Entity"*) para consultar a MIB do dispositivo tem de comunicar com o objeto a ser gerido. Esta comunicação é realizada utilizando o protocolo de comunicação SMNP.
Quando o gestor pretende saber se um determinado serviço, de um dispositivo de rede, se encontra ativo envia um pedido de consulta da MIB para o dispositivo, através do protocolo SMNP. Desta forma é obtido o resulta desta consulta à MIB e é enviada em forma de resposta para o gestor.

Em alguns dispositivos que não possuem MIB é possível instalar um agente que recolhe informações sobre o sistema, agente procurador. Estas informações depois podem ser consultadas da mesma forma, utilizando o protocolo SNMP.

2.4.2. Arquitetura descentralizada

A arquitetura descentralizada é utilizada em redes mais complexas e com um elevado número de objetos a serem geridos. Desta forma é necessária a utilização de uma abordagem diferente na gestão, com a mesma a ser deslocada para junto das entidades que se pretendem gerir.

Para estes casos, devido à necessidade de uma maior escalabilidade, a gestão descentralizada é a melhor opção. Nesta arquitetura existe uma distribuição de partes das tarefas de gestão pelos diversos agentes, tendo assim cada um destes, um certo grau de 'inteligência'. Dependendo das funcionalidades pretendidas no sistema é definido o grau e o tipo de descentralização. Dado a existência de uma maior capacidade de processamento dos dispositivos de rede, a arquitetura descentralizada tem vindo a ser cada vez mais implementada. Esta arquitetura traz algumas vantagens em sistemas que precisam de manipular grandes quantidades de informação e tem como resultado um conjunto mais reduzido de dados. Melhor escalabilidade, tolerância a falhas e processamento local são ainda mais valias desta arquitetura. A gestão remota aos dispositivos também é possível, mesmo com ligação aos agentes de baixo débito. As sondas RMON (*Remote Network Monitoring*) são a forma mais simples de monitorização remota descentralizada.

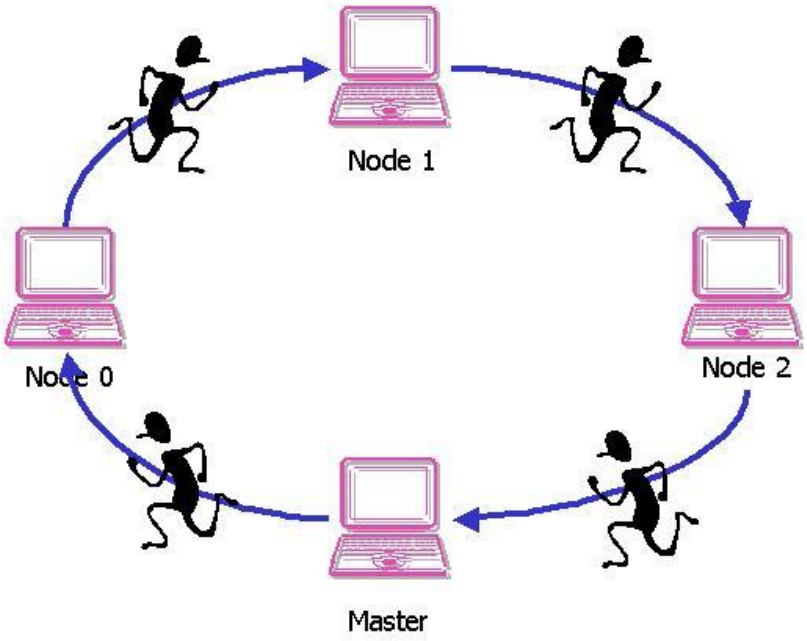


Figura 3 - Agentes Moveis. (Qi, 2001)

Numa arquitetura descentralizada são utilizados agentes móveis ao contrário da arquitetura centralizada.

Estes agentes são processos de *software* capazes de se deslocarem automaticamente de um local da rede para outro. O agente desloca-se para o objeto a ser gerido e executa o seu código para obtenção de informação ou execução de algum comando. Depois, automaticamente avança para outro objeto e executa novamente o código. Quando termina o seu percurso volta à entidade gestora para deixar um relatório das atividades efetuadas. O percurso e as funções que o agente deve exercer sobre os objetos são previamente configuradas na entidade gestora.

2.4.3. Modelo de informação de gestão

"The Management Information Base (MIB) is a conceptual data store that contains a management view of the device being managed. The conceptual data contained in this data store constitutes the management information.". (Alexander Clemm, 2006)

A MIB é um repositório conceptual de dados que contem uma perspetiva de gestão sobre o dispositivo que está a ser gerido. Os dados contidos nesse repositório constituem a gestão da informação. As operações de gestão são dirigidas contra esta "base de dados", por exemplo as portas de rede de um *switch* podem ser representadas numa tabela, em que cada porta tem uma entrada correspondente na tabela. As colunas no quadro conceptual contêm atributos que correspondem a propriedades reais do dispositivo. Exemplos de tais atributos são o tipo de protocolo de comunicação suportado pela porta e o número de pacotes transmitidos.

Uma MIB é uma estrutura de dados em árvore em que cada nó é representado por uma sequência de números (*ISO Object Identifier Tree*)

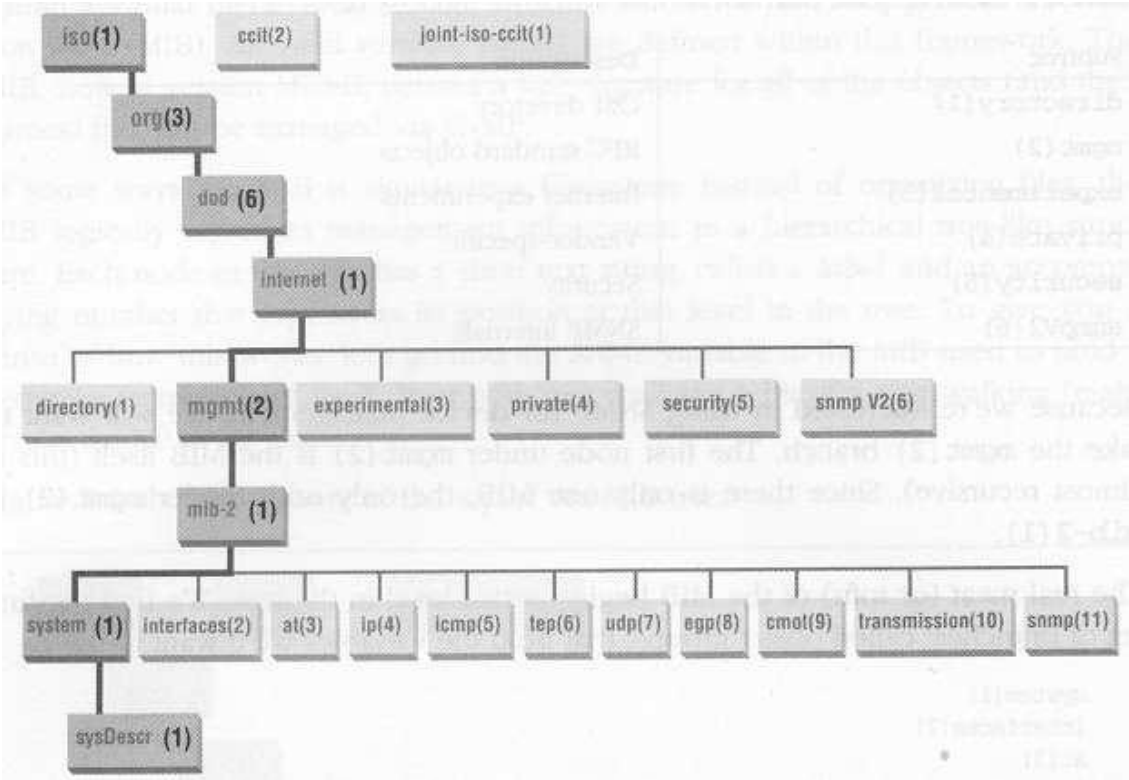


Figura 4 - Management Information Base. (Oreilly, 2009)

OID – *Object Identifier* é um conjunto de números separados por pontos que representa um nó da árvore. Por exemplo: SysDescr(1) tem o OID .1.3.6.1.2.1.1.1.0

Da consulta de um OID de uma MIB obtém-se como resultado um valor numérico ou texto.

2.4.4. SNMP (Simple Network Management Protocol)

O protocolo SNMP teve sua origem no SGMP ("*Simple Gateway Monitoring Protocol*").
Este protocolo começou muito simples e por este motivo foi rapidamente adotado.

O SNMP foi desenhado com vista a fornecer um conjunto simples de operações que permitia gerir dispositivos remotamente.

O protocolo SNMP utiliza como protocolo de transporte de dados o UDP (*User Datagram Protocol*) entre a entidade gestora e o objeto gerido. O protocolo UDP foi escolhido em vez do protocolo TCP porque em termos de ligação é mais simples, pois não necessita de uma verdadeira conexão entre os agentes envolvidos, isto é, quando é enviada informação não se está á espera de uma resposta de confirmação. São utilizados simplesmente *time-outs*. Caso a informação não chegue ao destino num determinado período de tempo o gestor volta a pedir a informação desejada.

O protocolo SNMP utiliza a porta UDP 161 para enviar informação e para receber utiliza a porta 162.

A maioria dos dispositivos de rede atuais suportam o protocolo SNMP.

Existem 3 versões deste protocolo.

- SNMPv1 e SNMPv2 – utiliza uma noção de comunicação de confiança entre gestor e agente. O agente é configurado com três *community names*: *read-only*, *read-write* e *trap*.
  Community name são essencialmente *passwords* e são utilizadas para aceder às MIB's.
  Communtiy String read-only – permite ler informação.
  Community String read-write – permite ler e modificar dados. Como limpar uma contagem.
  Communty String trap – Permite receber notificações assíncronas do agente.
  (Scbmidt, 2005)
  Não é utilizado qualquer tipo de codificação nestas versões.
- SNMPv3 – Nas versões anteriores a segurança, ou a falta dela, é a maior fraqueza do protocolo SNMP deste o início. A autenticação na versão v1 e v2 do protocolo não passa de uma simples *password* (*Community String*) enviada em texto sem codificação entre o gestor e o agente.
  A versão v3 deste protocolo vem colmatar este problema. É utilizada uma autenticação de tipo *User-Based* que usa algoritmos de autenticação, MD5 ou SHA, e DES como algoritmo de encriptação. Não existem outras modificações no protocolo com exceção da introdução de novas convecções textuais, conceitos e terminologias. A mudança mais importante é o

> abandono da noção de gestor e agente. Ambos passaram a ser denominados de entidades SNMP. (Scbmidt, 2005)

Como foi referido anteriormente, o SNMP consiste num protocolo simples que permite a uma estacão gestora inspecionar e modificar a informação de gestão de um elemento remoto de rede (agente), bem como o transporte de notificações geradas por estes. O protocolo especifica os seguintes tipos de operações:

Operação de leitura (GET) - permite consultar um determinado parâmetro de um agente;
Operação de atualização (SET) - permite modificar um determinado parâmetro de um agente;
Operação transversal (GET-NEXT) - permite consultar parâmetros de um determinado agente sem necessidade de conhecer a MIB que o agente implementa. A seleção do objeto a consultar é feita sobre a instância imediatamente posterior à anteriormente indicada.
Operação de notificação (TRAP) - permite a cada agente notificar a ocorrência de eventos extraordinários.

Das quatro operações apresentadas, três delas são confirmadas e tem origem no gestor (GET, GET-NEXT e SET) e apenas uma (TRAP) é gerada pelo agente e não tem confirmação.

O SNMP tem cinco PDUs ("*Protocol Data Units*") na base das suas operações:
GetRequest e **GetNextRequest**, utilizados na leitura de informação;
SetRequest, utilizado na modificação de valores;
Response, trama de resposta aos comandos anteriores;
Trap, utilizado pelo agente na notificação de eventos anormais.

A primeira versão do SNMP detém muitas deficiências, principalmente ao nível da segurança e das operações. Visando a eliminação destas deficiências, foi publicada uma atualização do SNMP, conhecido como SNMPv2 que foi enriquecido com duas novas operações:
Operação de informação - permite a troca de informação entre estações gestoras (INFORM);
Operação de consulta múltipla - semelhante à operação transversal (GET-NEXT) mas permitindo a especificação de múltiplos parâmetros (GET-BULK).
GET não atómico - a falha de consulta a uma variável não impede o comando de prosseguir com outras consultas.

Um protocolo de gestão deve ser seguro, particularmente em operações de atualização (SET). Deve admitir a extensão posterior de funcionalidade à medida que novos mecanismos ou protocolos surjam. Estes foram alguns dos objetivos patentes no desenvolvimento do SNMPv3. Acima de tudo, o SNMPv3 não deve apresentar rotura com o SNMPv2 ou o SNMPv1 facilitando a transição dos sistemas já instalados.

3. Aplicações de Monitoração

Existem várias aplicações de monitoração, algumas comerciais outras gratuitas, mas todas elas têm com o propósito efetuar gestão e monitorização de equipamentos de rede, utilizando o protocolo SNMP.

3.1.Aplicação HP Network Node Manager

O "*Hp Network Node Manager*" é uma aplicação de monitorização comercial. Trata-se de uma aplicação de gestão que tem a particularidade de possuir configurações prontas a serem utilizadas em qualquer rede. Permite gerir redes físicas e virtuais de qualquer tamanho, gerando a informação necessária para detetar e resolver qualquer tipo de problema.

As principais funcionalidades disponíveis são:

- Efetuar relatórios de estado e performance dos *links* entre dispositivos;
- Efetuar gestão de dispositivos de voz;
- Efetuar gestão de centrais telefónicas, tais como Cisco e Nortel;
- Monitorizar a qualidade da voz.

A figura seguinte mostra a consola da aplicação, onde o administrador pode obter todas as informações de gestão assim como despoletar ações de gestão.

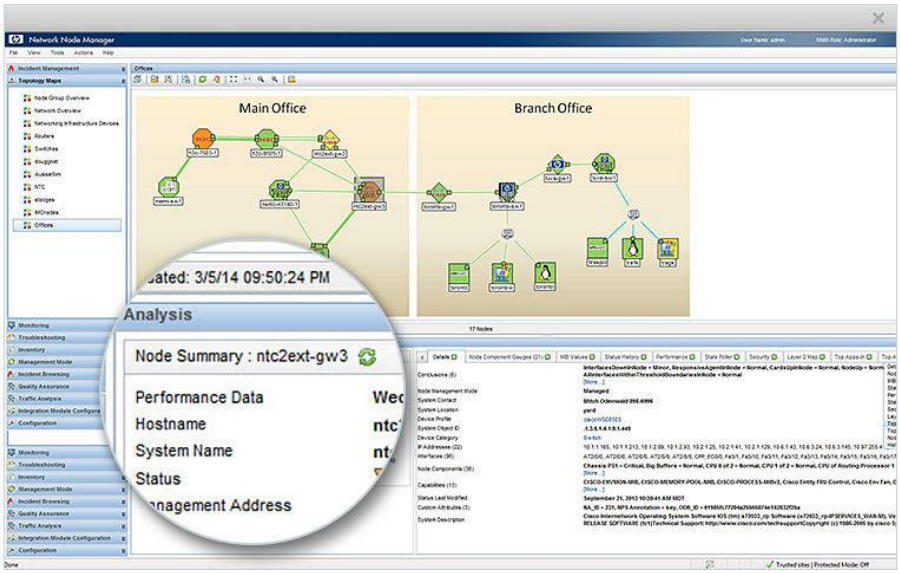


Figura 5 – NNMI. (NNMI, 2015)

3.2.Nagios

"Nagios" é uma aplicação de gestão gratuita. As suas características e funcionalidades são muito semelhantes às das aplicações comerciais disponíveis no mercado.

É considerada uma das melhores aplicações gratuitas disponíveis para monitorização de redes. É uma ferramenta modular que faz com que seja mais fácil monitorizar redes com elevada escalabilidade.

O "Nagios" não é uma aplicação pronta a ser utilizada, isto é o gestor de rede tem de configurar cada dispositivo a ser monitorizados nos ficheiros de configuração do Nagios. Cada rede é única e não existe uma solução pronta para todas as redes. É necessário 'ensinar' o "Nagios" a monitorizar cada dispositivo, cada serviço, cada ação.

O "Nagios" não é nada amigável para quem esta a começar. É uma ferramenta que requer muito esforço para ser instalado e configurado adequadamente.

A figura seguinte ilustra o resultado obtido quando se faz uma pesquisa da rede com o "Nagios".

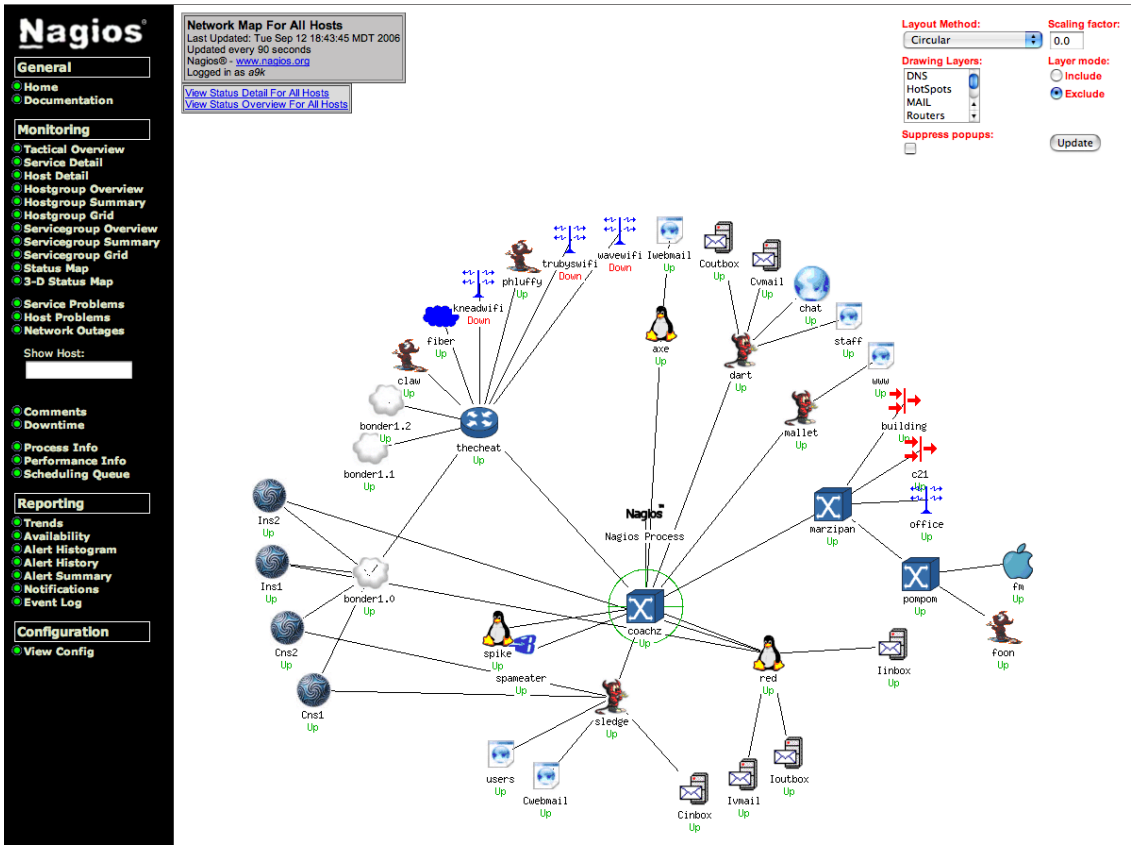


Figura 6 - Exemplo do map no “Nagios”. (NagiosMap, 2006)

O “Nagios” possuí as seguintes funcionalidades:

- Capacidade para **c**onfigurar cada um dos dispositivos;
- Capacidade para agrupar tipos de dispositivos;
- Capacidade para agrupar serviços;
- Geração de alertas através de envio de *emails* para os administradores de rede.

A aplicação permite ainda monitorizar diversos serviços, tais como serviços SMTP, POP3, HTTP, NNTP, ICMP, SNMP entre outros.

A aplicação disponibiliza, ainda a possibilidade do administrador de rede criar os seus próprios *plugins* para serem utilizados pelo “Nagios”.

3.3.Icinga

"Icinga" é uma aplicação para monitorização de redes e sistemas que nasceu em 2009 semelhante ao "Nagios". Em 2012 foi criada uma nova versão que é mantida em paralelo com a versão inicial, chamada de "Icinga2", desenhada para monitorizar ambientes mais complexos e de maior dimensão, com *interfaces* novos e com a capacidade de monitorização distribuída.

A arquitetura do "Icinga" é composta por três componentes que funcionam em paralelo: "Icinga Core", "Icinga Web" e IDODB (*Icinga Data Out Database*). A componente "Icinga Core" gere as tarefas de monitorização, recebendo os resultados das verificações dos diversos *plugins*, e enviando esses resultados para a base de dados (IDODB) através do *interface* IDOMOD e do serviço IDO2DB. O "Icinga Web" é a *interface* principal, onde é possível visualizar os resultados das verificações e enviar comandos para o "Icinga Core". Por último, a IDODB é a base de dados onde é guardada toda a informação recolhida do estado dos *hosts*.

Principais características e funcionalidades:

- Regras de configuração simples;
- Possível e fácil migração do "Nagios" para o "Icinga";
- Comandos interessantes e objetivos como o "*assign Where*" ou "*ignore where*".

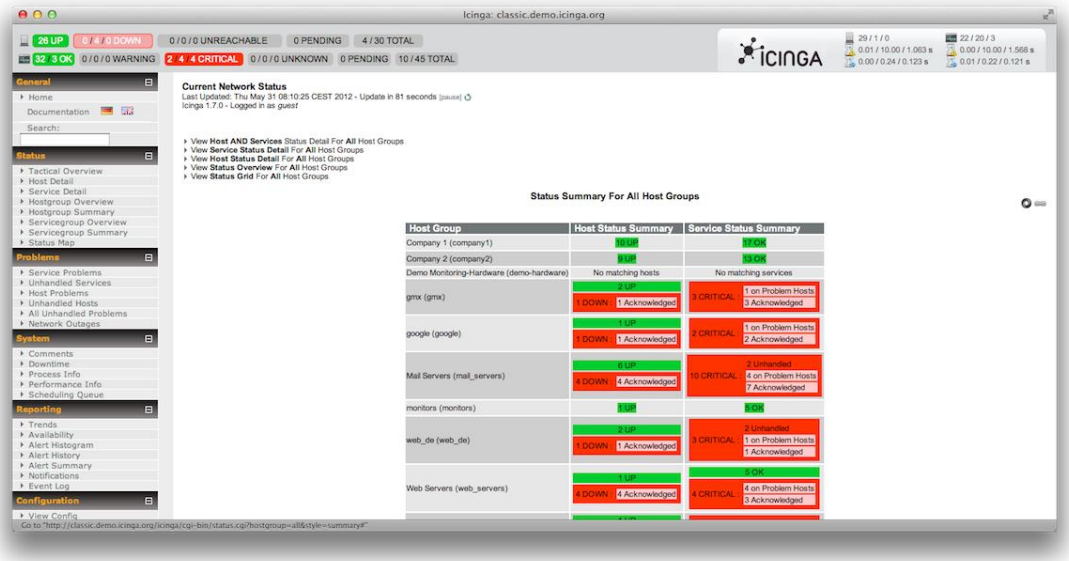


Figura 7 - *ScreenShot* do "Icinga". (Icinga, 2014)

Da observação da figura anterior pode-se verificar que em termos gráficos realmente é muito semelhante à aplicação "Nagios". No entanto, esta aplicação possui algumas desvantagens das quais destacamos as seguintes:

O "Nagios" é um sistema muito mais flexível do que o "icinga". "*Nagios has been monitoring our systems for the last couple of years and the amount of flexibility that it has given us is amazing*. " – *Systems Administrator, Gulf Research Center* (Nagios_vs_Icinga, 2011)
O "Nagios" é um sistema muito mais proactivo. "*Nagios rocks. We've been using it in production and it has definitely allows us to get better look at things as well as be much more proactive to network issues.* " – CTO, pvbb.net (Nagios_vs_Icinga, 2011)

3.4.Opsview

"Opsview" é uma aplicação empresarial de gestão. Desta aplicação destacamos as seguintes funcionalidades:

- *Auto-discovery* – A aplicação é capaz de descobrir os equipamentos de rede automaticamente;
- Possui um interface gráfico amigável;
- Facilidade na configuração, minimizando o trabalho manual devido à disponibilidade de *auto-discovery;*
- Possibilidade de organizar os equipamentos e as aplicações por grupos;
- Capacidade de efetuar monitorização por grupos;
- Visualização gráfica muito poderosa.

As figuras seguintes permitem visualizar algumas das janelas disponíveis na aplicação.

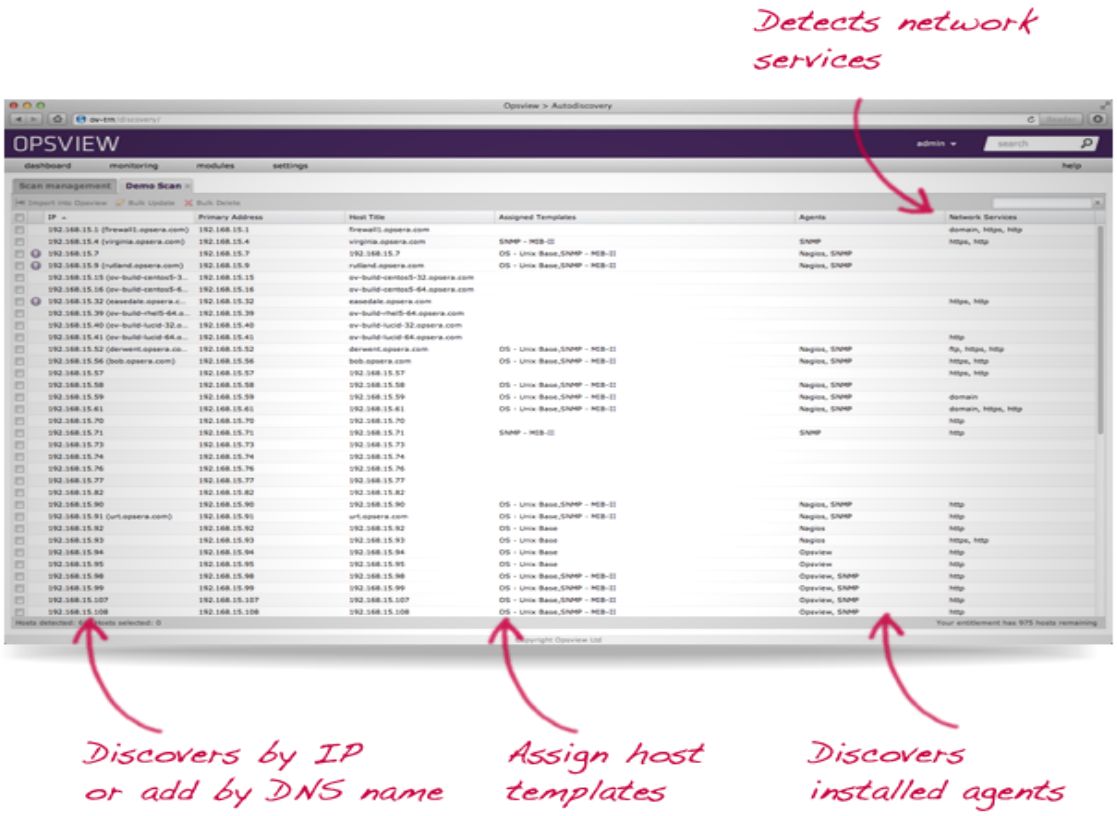


Figura 8 - *Screenshot* do *auto-discovery* (Opsview, 2015)

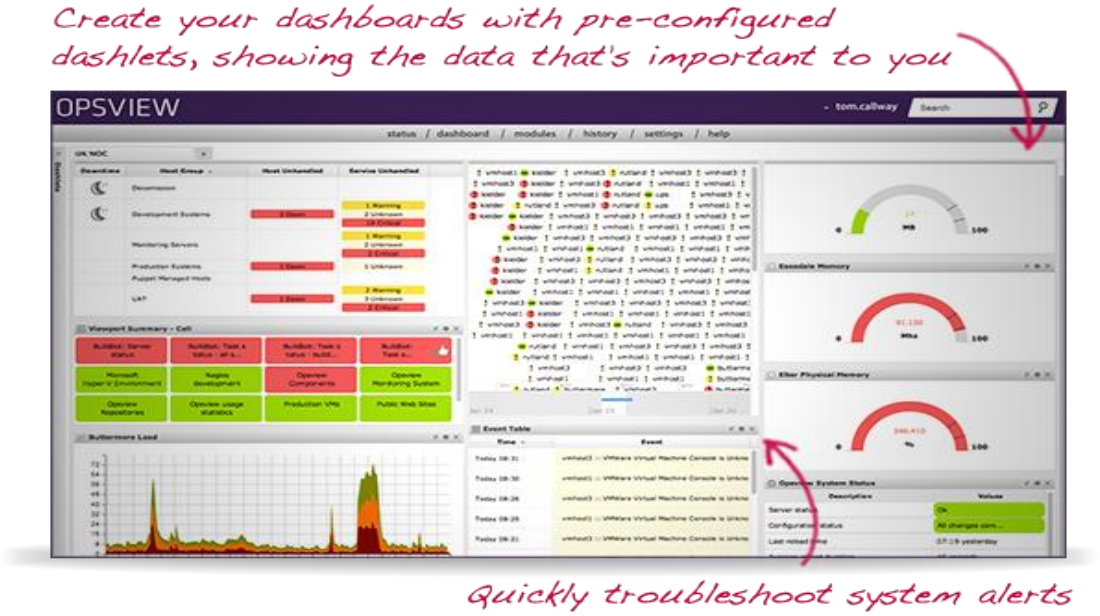


Figura 9 – *Dashboard* (Opsview, 2015)

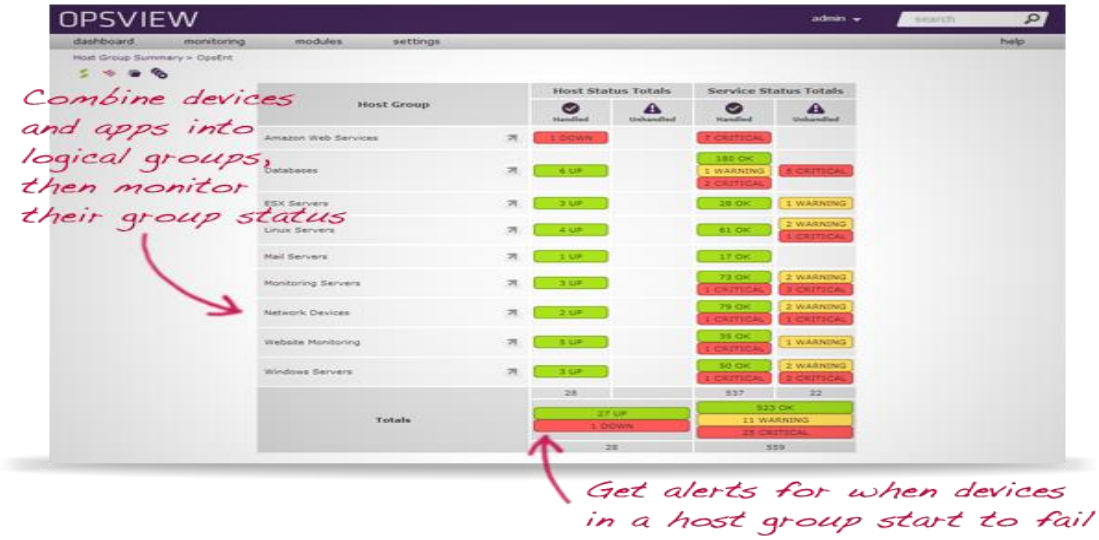


Figura 10 – "OpsView" *Groups* (Opsview, 2015)

O Sistema de monitorização *Open Source* "Opsview's" foi desenhado para ser um Sistema flexível e de fácil utilização. Baseado no Sistema de monitorização "Nagios" a sua instalação, configuração e atualização para o "Opsview's" não requer conhecimentos especializados ou despesas adicionais num especialista. É essencialmente necessário ter um técnico para monitorizar a performance da atividade dos dispositivos e dos serviços, assim como verificar os alertas gerados, procedendo à resolução dos problemas ocorridos (Opsview Development Team, 2011).

Ao contrário das soluções proprietárias a versão comercial da "Opsview's" oferece condições especiais para qualquer tipo de empresa, grande ou pequena. Possui uma grande equipa de especialistas que proporcionam suporte profissional cobrindo todos tipos de monitorização sem qualquer perda de privilégios ao longo dos anos. (Opsview Development Team, 2011)

3.5.Multi Router Traffic Grapher (MRTG)

"MRTG" é uma ferramenta que monitoriza o tráfego nos *links* numa infraestrutura de rede. Inicialmente a ferramenta "MRTG" teria a função de obter dados dos *routers* utilizando o protocolo SNMP e apresentar os dados ao administrador de rede de uma forma simples e de fácil compreensão.

No entanto, esta ferramenta tornou-se capaz de apresentar qualquer tipo de dados numéricos obtidos de qualquer equipamento.

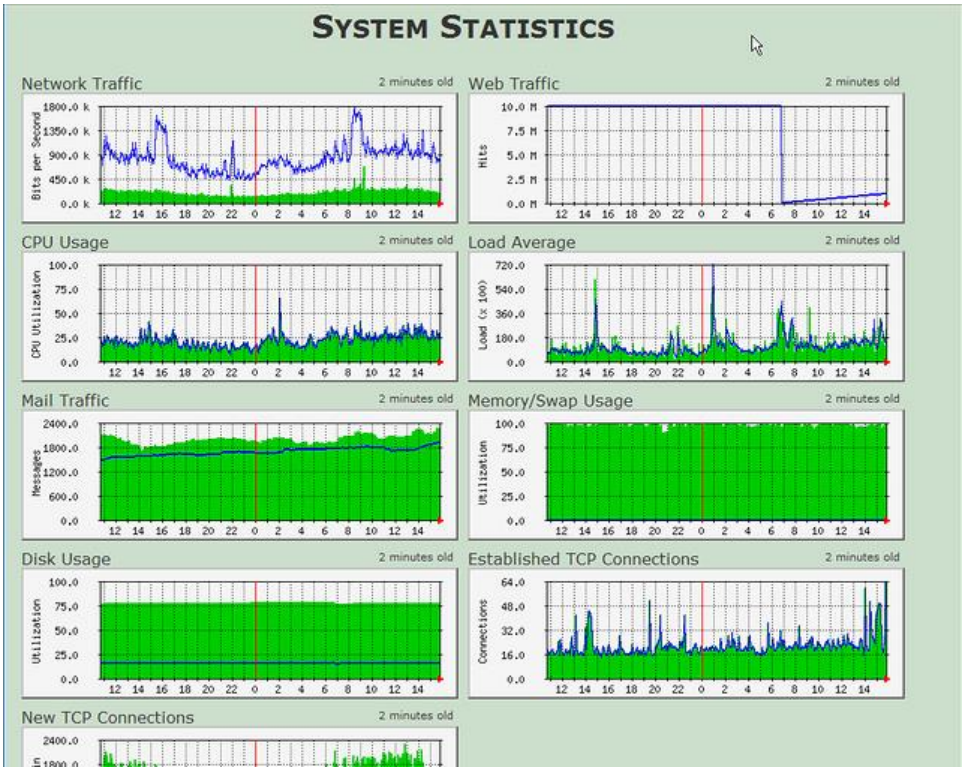


Figura 11 - Exemplo "MRTG" (mrtg, 2015)

Na figura anterior é apresentado um exemplo de dados obtidos pelo script da aplicação "MRTG". Estes dados são tratados e apresentados num formato HTML. O administrador de rede pode ler os gráficos de forma a retirar as conclusões necessárias relativamente à largura de banda ocupada pelos *links*, consumo de memória pelos sistemas, capacidades dos discos, etc. A grande vantagem é a possibilidade de ter um histórico do comportamento destes recursos.

O relatório de tráfego para um determinado *link* pode ser apresentado em quatro gráficos: diário, última semana, últimas cinco semanas e último ano.

As principais características da aplicação são:

- Capacidade para monitorizar tráfego;
- Capacidade para ler os valores, via protocolo SNMP (*Simple Network Management Protocol*), ou através de scripts;
- Disponibilização da ferramenta CFGMAKER, que permite gerar facilmente os ficheiros de configuração do "MRTG";

- Disponibilização da ferramenta INDEXMAKER para gerar páginas de índices (no caso de termos muitas interfaces a serem monitorizadas).

O "MRTG" é uma ferramenta poderosa e muito útil para qualquer administrador de uma rede. Através da informação produzida podemos ter informação sobre a realidade da rede, assim como a possibilidade de detetar eventuais "picos" na utilização da mesma.

3.6.PNP4Nagios

O "PNP4Nagios" é um *addon*, em linguagem PERL, PHP e C para o "Nagios", que analisa os dados de performance provenientes dos *plugins* do Nagios e grava-os em base de dados RRD "*Round Robin Database*". Esta ferramenta possui funcionalidades que lhe permitem criar gráficos sobre a utilização da CPU, da Memória, da Largura de banda, entre outras As figuras seguintes permitem visualizar a aplicação.

Algumas das características e funcionalidades da aplicação são:

- Trata-se de uma ferramenta pronta a ser utilizada sem necessitar de grandes configurações;
- Estar desenhada para ser utilizada com o "Nagios" e com os seus *plugins*;
- Permite criar gráficos automaticamente.

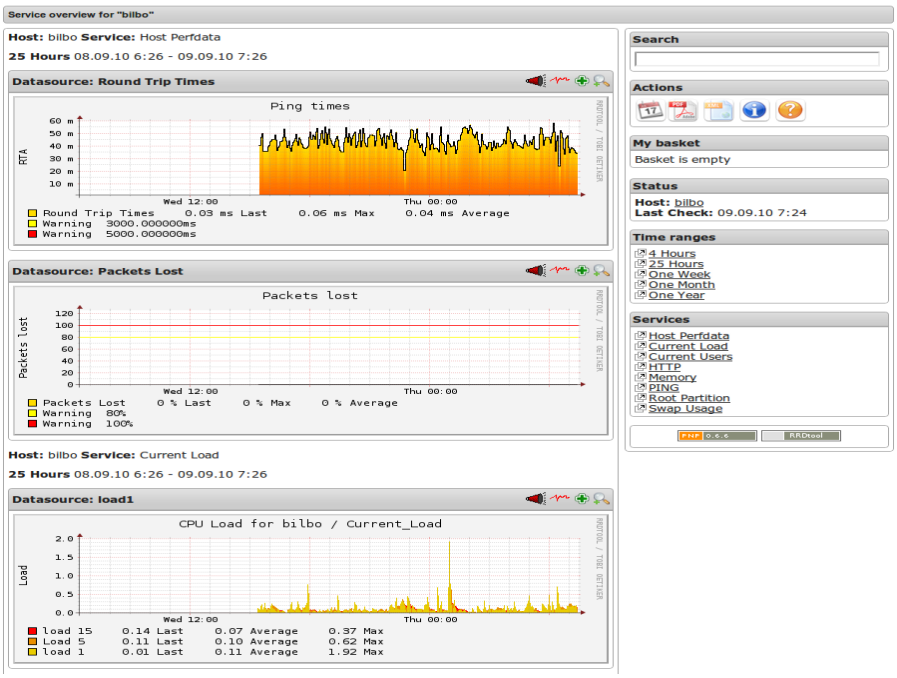


Figura 12 - Exemplo do "pnp4Nagios". (PNP4Nagios, 2010)

3.7.Outras aplicações de monitorização não SNMP

3.7.1. NTOPNG

"NTOPNG" é uma aplicação de análise de tráfego numa rede. Na página oficial desta aplicação pode-se consultar as suas principais funcionalidades (NTOPNG, 2015), das quais destacamos

- Capacidade para ordenar o tráfego na rede pelos vários protocolos presentes;
- Mostrar os *hosts* ativos na rede. Tanto em IPv4 como em IPv6;
- Armazenar em disco, estatísticas de tráfego;
- Efetuar geolocalização dos *hosts*;
- Mostrar o tráfego IP de acordo com os vários protocolos;
- Analisar e ordenar o tráfego de acordo com o emissor ou destinatário.

Por defeito, o "NTOPNG" utiliza as camadas 2 e 3 do modelo OSI. *Media Access Control* (MAC) e TCP/IP.

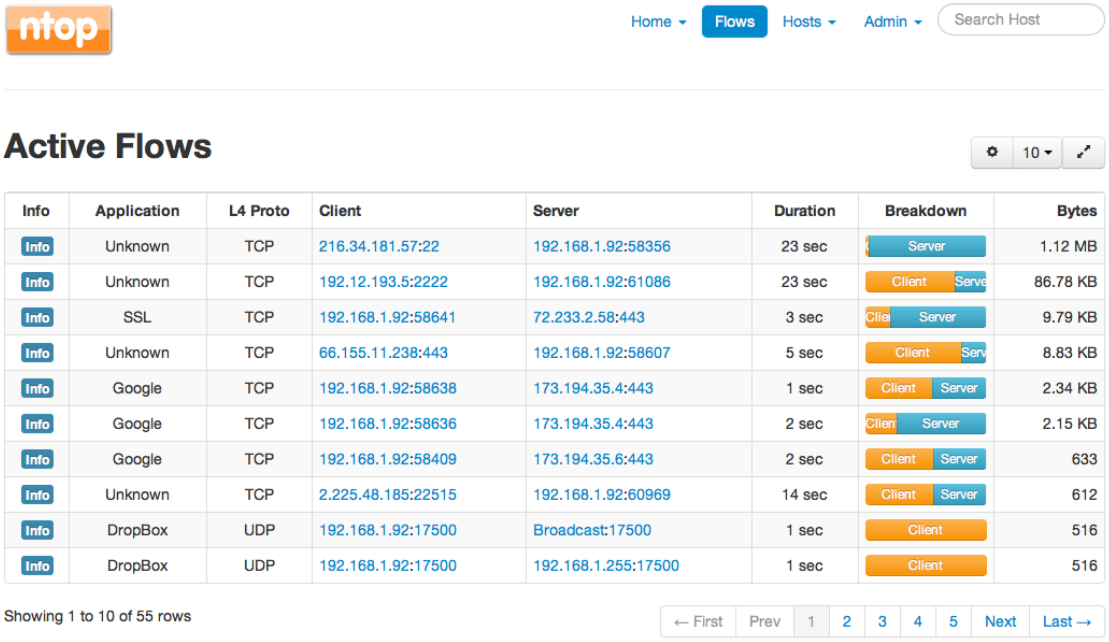


Figura 13 - Exemplo "NTOPNG" (NTOPNG, 2015)

Na figura anterior pode-se verificar que com esta aplicação é possível analisar o tráfego, em tempo real, que circula numa rede. Com esta análise é possível verificar onde, ou quem está a consumir largura de banda que não deveria, ou a utilizar protocolos de comunicação que congestionam o bom funcionamento de rede.

Esses protocolos de comunicação podem estar a ser utilizados intencionalmente pelo cliente, ou podem ser aplicações maliciosas, no cliente, a utilizarem recursos da rede que não é suposto.

3.7.2. OCS-Inventory

"OCS-Iventory" é uma aplicação web que permite aos administradores de rede obter informações relevantes dos computadores de uma organização. Esta aplicação necessita que em cada computador seja instalado um agente. Ele é responsável por enviar informações e detalhes para um servidor MySQL. O *"OCS-inventory"* consulta as tabelas no servidor MySQL e disponibiliza essa informação em formato *web*.

Das informações enviadas pelo agente destacamos as seguintes: Deteção de computadores e máquinas virtuais, Discos/Partições/memória assim como os respetivos detalhes; Sistemas operativos; *Software* instalado; Descrição do computador, etc.

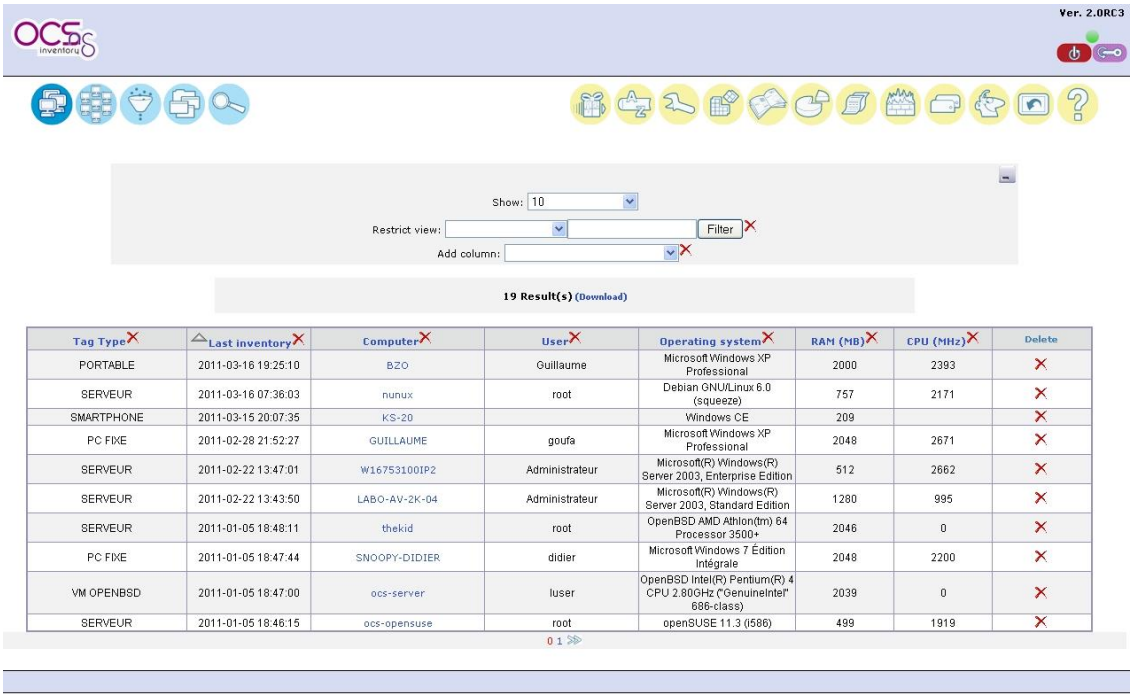


Figura 14 – OCS-Iventory (OCS Iventory, 2014)

Na figura anterior pode-se verificar como são apresentadas todas as informações relativas aos computadores que constituem uma rede estruturada. Esta informação pode ser consultada na página oficial da aplicação. (OCS Iventory, 2014)

4. Arquitetura de Rede e Serviços na Câmara Municipal de Santo Tirso

4.1.Introdução

A Câmara Municipal de Santo Tirso está localizada num edifício antigo. A Câmara é constituída por vários departamentos, divisões e serviços. Alguns destes serviços estão localizados em edifícios distantes do edifício da Câmara.

4.2.Caracterização da Rede

O edifício da Câmara possui três pisos, três departamentos, cinco divisões e dezasseis serviços.

O Serviço de Informática está localizado no piso -1, onde ocupa dois espaços distintos. No primeiro espaço encontram-se instalados o bastidor de servidores e o bastidor de rede. No segundo espaço está localizada a equipa de informática que é constituída por seis técnicos, com diversas funções que na prática permitem a resolução dos vários problemas que ocorrem no dia-a-dia da organização.

No bastidor de rede existem dois *routers*, onde um conecta a rede interna à fibra e o outro a uma linha de auxiliar *adsl*, três *switches*, sendo que dois com portas de acesso para as conexões aos servidores e dispositivos de rede que se encontram nesse piso, e um *switch* na camada *core* para as conexões de fibra até aos vários *switches* distribuídos pelo edifício da Câmara. Existem três ligações de fibra para edifícios distantes fisicamente do edifício da Câmara.

A rede estruturada de dados da Câmara está configurada da seguinte forma:

- Duas Ligações externas, uma em fibra, e uma em *adsl*;
- Uma única *vlan,* com IP de rede 10.1.0.0/16;
- Um *Switch* da camada core – Catalyst 4000 L3 (WS-C4507R);
- Cinco *Switches* de acesso – Catalyst 2960 (WS-C2960G-48TC-L);
- Onze *Switches* de acesso – Catalyst 500 (WS-CE500-24LC);
- Quatro *Switches* de acesso.

Servidores, multifunções e computadores:

- Quatro Servidores com sistema operativo *Linux*;
- Doze Servidores *Windows*, sendo três virtualizados;

- Quinze Multifunções;
- Duzentos e quarenta e seis Computadores inventariados.

4.3.Topologia de Rede

A rede interna dos computadores e servidores é a 10.1.0.0/16, dos *swicthes* é 172.16.10.0/24.

Como se pode verificar em vez de ser configurado *vlan's* diferentes para os computadores, servidores, *swithces* e impressoras foi decidido utilizar uma única *vlan* para todos equipamentos. Utiliza-se IP's secundários no *switch* 4507 para que a rede 10.1.0.0 comunique com a rede de gestão dos *switches,* 172.16.10.0.

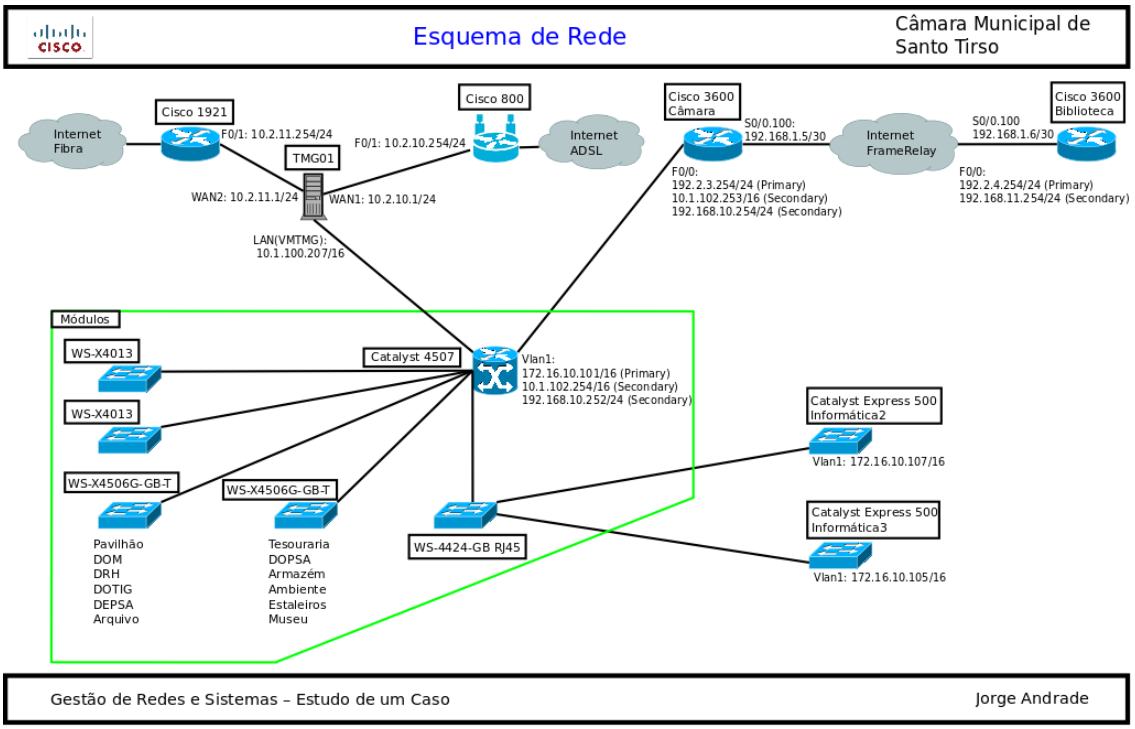


Figura 15 - Topologia de Rede – Bastidor de rede

A figura 16 mostra que o equipamento central desta rede é o Servidor TMG ("*Threat Management Gateway"*). Este servidor é responsável pela gestão das comunicações tal como um *router*. A *default Gateway no Catalyst* 4507 é o tmg – 10.1.100.207.

Este *switch* faz os *link's* de fibra com os *swicthes* L2 indicados na imagem.

O *switch* "Informatica2" e "informatica3" são de acesso aos computadores.

Foi configurado uma ligação *frame-relay* da Câmara para a Biblioteca porque são edifícios distantes. Com esta ligação é possível fazer o sincronismo da *Active Directory* com um servidor instalado na Biblioteca Municipal.

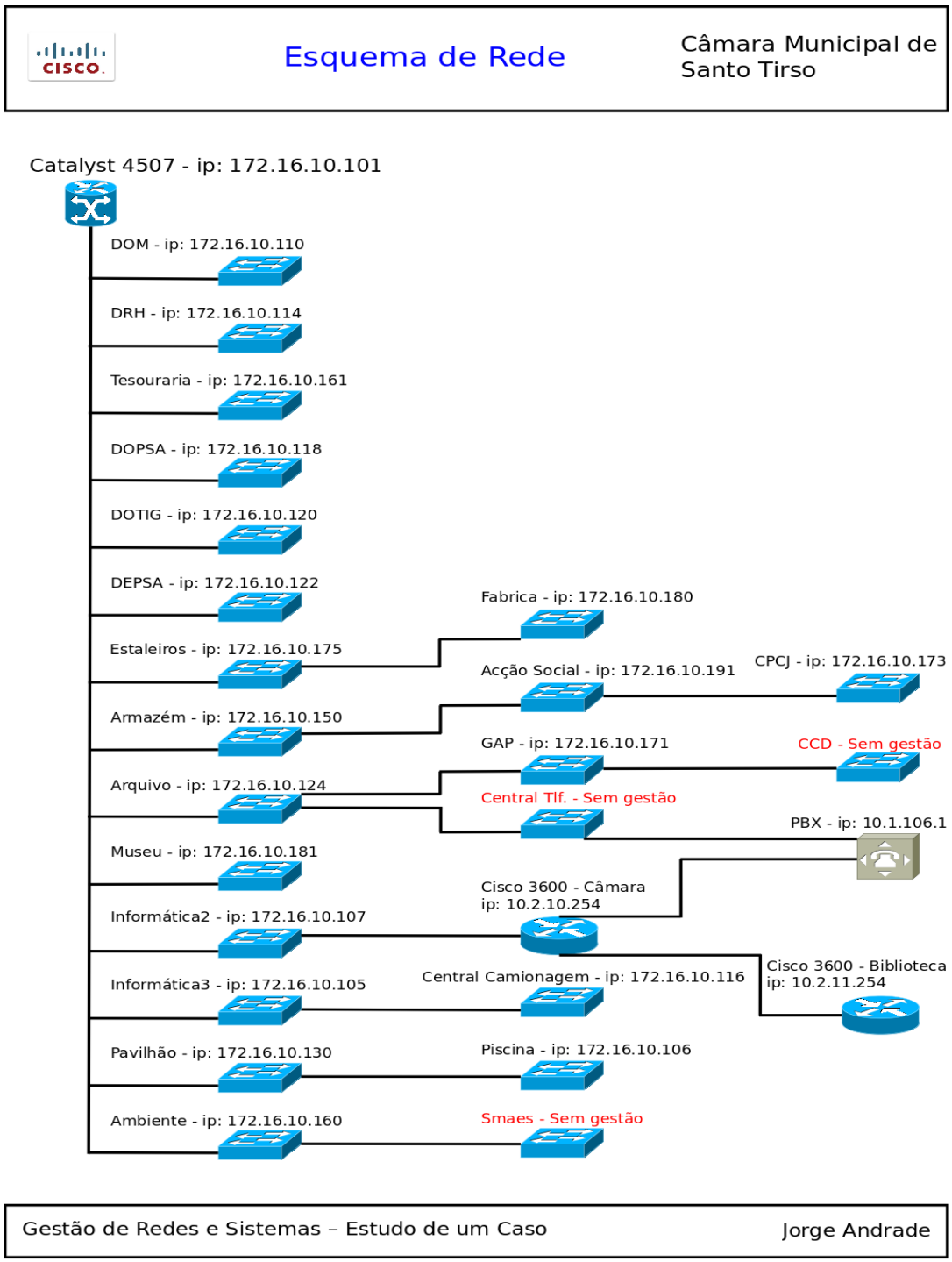


Figura 16 - Esquema de rede

A figura 17 apresenta a quantidade de equipamentos ativos de rede na Câmara Municipal de Santo Tirso. Através deste levantamento sobre os dispositivos a serem monitorizados verifica-se que na Câmara existe um grande número de equipamentos e que a probabilidade de falhas, quer do próprio equipamento, ou humanas, são elevadas.

Com este desenho e arquitetura de rede tornar-se muito difícil descobrir de forma atempada alguma anomalia que esteja a acontecer num determinado momento. Conclui-se que é fulcral e absolutamente necessário a implementação de um sistema de monitorização com a capacidade de gerar alertas aos técnicos e administradores de rede.

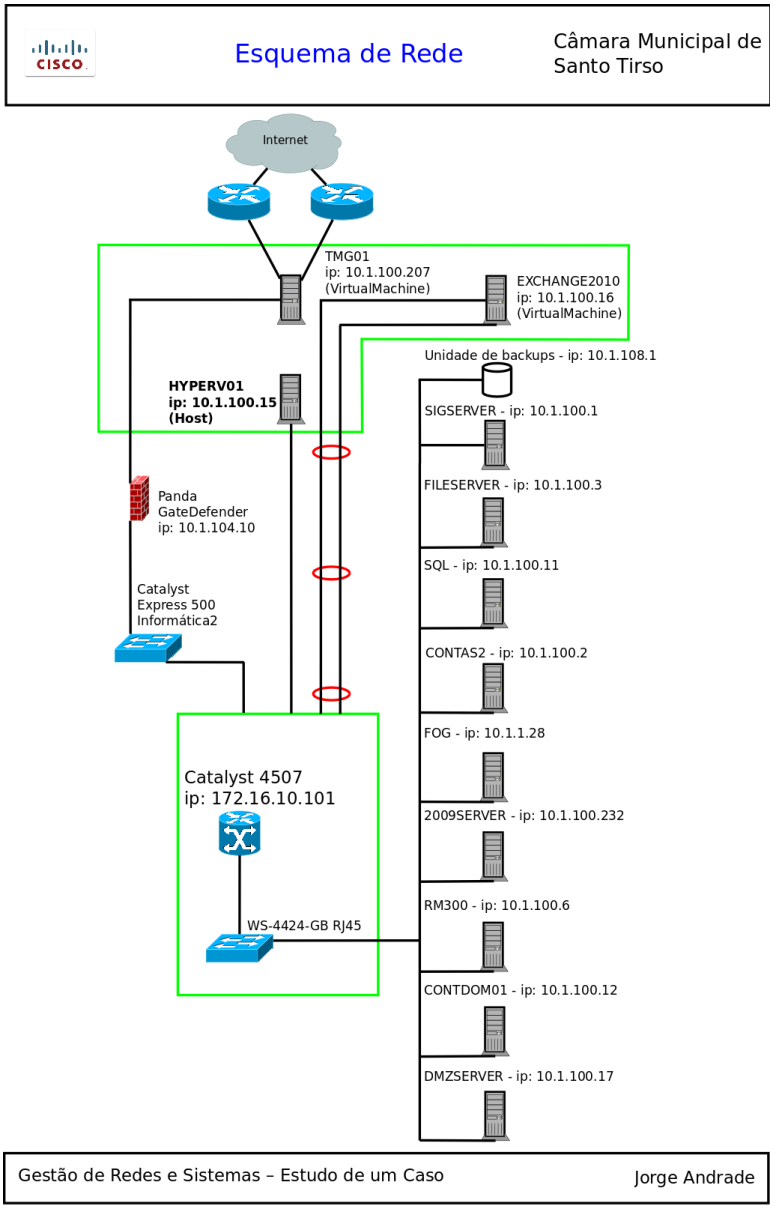


Figura 17 - Diagrama de rede (Servidores)

Na figura anterior é possível verificar quais os servidores que se encontram na Câmara. O servidor "Hyperv01" possui duas máquinas virtuais, O Servidor de Exchange e o TMG.

O Servidor TMG, apesar de ser virtual, utiliza duas portas físicas do "Hyperv01" para fazer o roteamento dos pacotes entre o *router* e o "Panda". O servidor virtual "Exchange2010" utiliza duas portas físicas agregadas do "Hyperv01" para a gestão de envio e receção de emails.

O servidor "Hyperv01" está fisicamente ligado ao *swicth* 4500.

O "panda gatedefender" é um equipamento de "UTM" ("*Unified threat management*"), trata-se de uma evolução das tradicionais *firewalls*.

"Today's continuing application explosion means that every day, more apps appear that traditional firewalls can neither detect nor control. Yet, establishing and maintaining control is not only desirable but is also downright essential because unchecked applications can wreak havoc. Web-based applications, because they pass unchecked through legacy firewalls, may not only import malicious or unwanted behavior and content onto an organization's networks, but they also may export proprietary, regulated, or confidential data out of its networks as well." (Ed Tittel, 2012)

Hoje em dia é fundamental a utilização deste tipo de equipamento numa organização que possui informação sensível e que a sua perda pode comprometer a credibilidade dessa organização.
Num organismo público essa preocupação tem de estar sempre presente porque a informação que circula é muitas vezes dos próprios munícipes que confiam os seus dados pessoais e assuntos confidenciais a estas instituições.

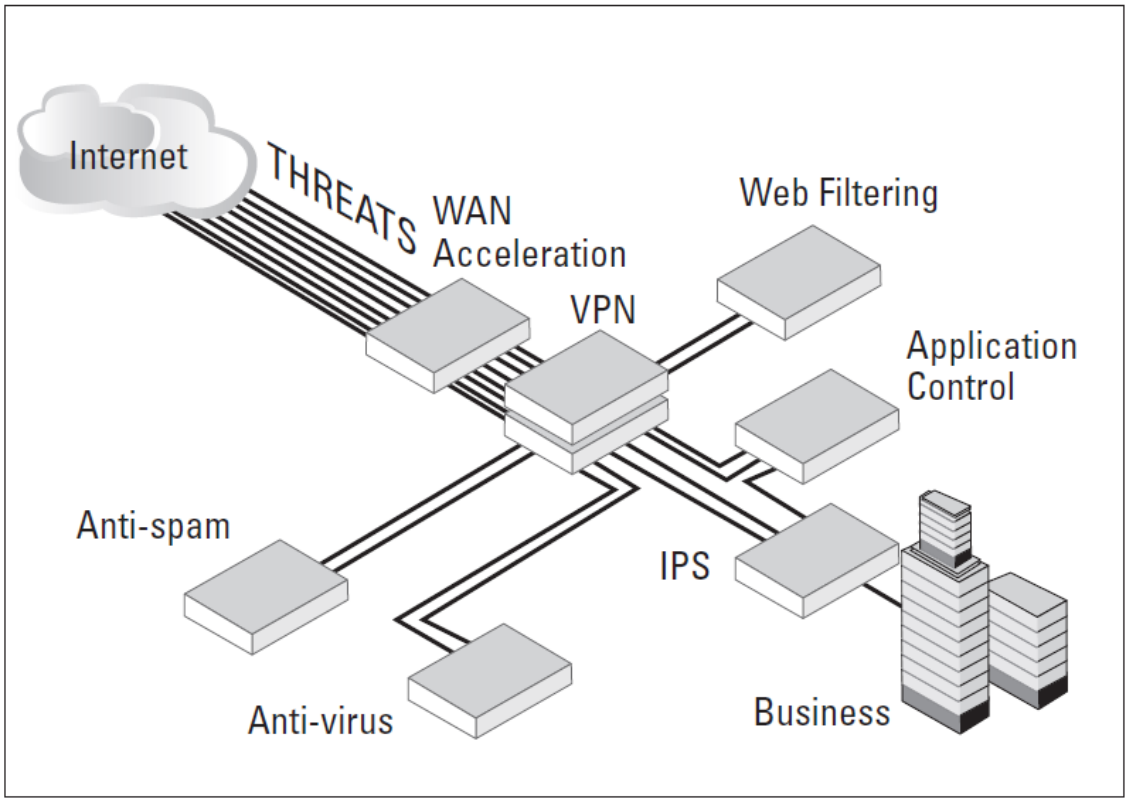


Figura 18 - Sistema multi aplicacional de proteção. (Ed Tittel, 2012)

A figura anterior permite verificar que num sistema tradicional de *firewall* são necessários todos estes equipamentos e aplicações do tipo servidor para ser possível efetuar um controlo dos dados que poderiam chegar até aos seus destinatários. Sendo que em muitas situações as mesmas verificações são repetidas, por diferentes aplicações, pelo facto de essas aplicações não comunicarem entre si.

UTM é uma mudança significativa na evolução da segurança tecnológica das redes e equipamentos. UTM refere-se a uma aplicação de segurança que consolida algumas funcionalidades essenciais de segurança num único equipamento, incluindo a próxima geração de tecnologias de *firewall* como aplicações de controlo. (Ed Tittel, 2012)

O "Panda GateDefender" no desenho da de rede da Câmara tem proteção contra *malware* e *spam*.

Como a default *route* do *switch* 4507 é 0.0.0.0 0.0.0.0 10.1.100.207 faz com que o tráfego passe de forma transparente pelo panda para ser analisado até chegar ao TMG. O TMG tem as seguintes funções que poderiam ser feitas pelo Panda:

- http/https Proxy Caching;
- Proteção e controlo de acesso à internet.

4.4.Servidores e Serviços

A Câmara municipal de Santo Tirso possui um domínio "cmst.local" onde todos os computadores e servidores se encontram adicionados. Este domínio possui dois controladores de domínio:

- "contdom01":
  - *Windows Server 2008 R2 Standard*;
  - Nível de funcionamento do domínio é o "*Windows Server 2008*";
  - Nível de funcionamento da floresta do domínio é o "*Windows Server 2003*";
  - DNS Secundário;
  - Mestre de operações (RID, PDC e *Infrastructure*).
- "fileserver":
  - *Windows Server 2003 R2*;
  - Nível de funcionamento do domínio é o "*Windows Server 2008*";
  - Nível de funcionamento da floresta do domínio é o "*Windows Server 2003*";
  - DNS Primário;
  - DHCP.

No controlador de domínio "contdom01" estão configurados todos os utilizadores do domínio, cerca de quatrocentos. Estes utilizadores estão agrupados de acordo com o serviço a que pertencem. As políticas de grupo também são configuradas neste servidor.

Para ser possível fazer uma boa gestão dos serviços a serem monitorizados foi necessário realizar um análise a cada um dos servidores e selecionar quais os serviços mais críticos para que fosse garantido o bom funcionamento das aplicações de rede.

Como nesta rede não existe uma configuração de redes logicamente separadas, *vlan's*, optou-se por criar reservas de IP's no DHCP por tipo de equipamento.
Na configuração do DHCP excluiu-se todos dos IP's disponíveis na gama de rede 10.1.0.0/16.
A cada equipamento introduzido na rede é necessário, manualmente, introduzir uma reserva com o respetivo endereço MAC da placa de rede do equipamento.

O Quadro seguinte mostra como estão distribuídas as reservas de IP's por equipamento.

Range de IP's	Equipamentos
10.1.0.1 – 10.1.99.253	Computadores
10.1.101.0 – 10.1.101.253	Impressoras de rede
10.1.100.1 – 10.1.100.253	Servidores

Tabela 1 - Reservas de IP's no DHCP

A monitorização atualmente é feita pelo TMG, onde são configuradas regras de acesso e permissões para cada um destes intervalos de endereços de rede. Constata-se que a rede suporta um total de 65534 *hosts*.

Porque não monitorizar todos os serviços?

A monitorização de todos os serviços de todos os servidores não é necessária nem é correta porque iria gerar tráfego desnecessário na rede. O importante é garantir o funcionamento dos serviços das aplicações de rede para que estejam sempre disponíveis. Sendo considerado mais importante a monitorização do próprio servidor, isto é, para que as aplicações estejam disponíveis é necessário que o servidor esteja comunicável e com o sistema operativo em funcionamento.

Após ter sido realizado um estudo e análise dos serviços a monitorizar foram criados os seguintes quadros:

Servidores	Descrição
Fileserver IP:10.1.100.3	• Controlador de domínio • Servidor responsável pela gestão do domínio e DNS primário • Também é utilizado com um servidor de ficheiro onde estão localizadas as pastas partilhados dos utilizadores
Sigserver IP:10.1.100.1	• Estão instaladas as bases de dados da aplicação "Gismat"
Hyperv01 IP:10.1.100.15	• Servidor com máquinas virtuais. "Exchange2010" e "TMG"
SQL IP:10.1.100.11	• Estão instaladas as aplicações de rede da medidata. Atendimento, Ciclomotores, Pocal, Cemitérios, Feiras, Fiscalização, Lixos, Obras Particulares, Obras Municipais, Publicidade, Rendas, etc.

Contas2 IP:10.1.2	• Está instalada uma aplicação *web* de gestão documental iPortalDoc – Sistemas de Gestão Documental
Fog IP:10.1.1.28	• OCS-Inventory – Aplicação *web* de inventário dos computadores no domínio da Câmara
Exchange2010 IP:10.1.100.16	• Está instalado o servidor de *email*. "Exchange 2010"
Tmg IP:10.1.100.207	• "Thret Management Gateway". Responsável pela monitorização e roteamento dos acessos internos e externos. • *Proxy* http e https
2009server IP:10.1.100.232	• "*Windows Server Update Services*". Disponibiliza os *updates* necessários aos computadores das ferramentas Microsoft • "*Windows Deployment Services*". Disponibiliza imagens "*Bare Metal*" para instalação em rede de sistemas operativos
Contodom01 IP:10.1.100.12	• Controlador de domínio • DNS secundário
Dmzserver IP:10.1.100.17	• Suporta o sistema de informação geográfico • Toponímia • Cartografia

Tabela 2 - Aplicações e funcionalidades dos Servidores

A monitorização de serviços em execução nos servidores é também uma tarefa essencial num sistema de monitorização de rede. No sistema da Câmara Municipal o "Nagios" terá a tarefa de monitorizar alguns desses serviços nos servidores.

Foram definidos os seguintes serviços para serem monitorizados pela ferramenta "Nagios".

Servidor	Serviços
Fileserver	• Active Directory Domain Services • DNS Server • File Services • Internet Information Services • Dynamic Host Configuration Protocol • Windows Internet Name Service

	• Hp Insight Server Agents • Panda Antivirus Service
Sigserver	• Internet Information Services • File Services • Hp Insight Server Agents • MapGuide Server 2.4 • Panda Antivirus Service • Postgresql-8.4
Hyperv01	• File service • Hyper-V • Hp Insight Server Agents • Hyper-V Networking Management Service • Panda Antivirus Service
SQL	• Autodes MapGuide Server 6.5 • Hp Insight Server Agents • MapGuide LightView6.5 • Panda Antivirus Service • Internet Information Services • SQL Server (MSSQLSERV) • SQL SERVER (SMAES)
Contas2	• http • IMAP • SMTP
FOG	• Smbd • Sendmail-mta • Sshd • Mysqld • /usr/bin/apach • Postgres
Exchange2010	• Active Directory Certificate Services

	• Background Intelligent Transfer Service • Hyper-V HearBeat Service • IIS Admin Service • Microsoft Exchange Active Directory Topology • Microsoft Forefront Server Protection Controller
TMG01	• Hyper-v HeartBeat Service • Microsoft Forefront TMG Control • Microsoft Forefront TMG Firewall • Panda Antivirus Service • SQL Server (ISARS) • SQL Server (MSFW)
2009server	• Background Intelligent Transfer Service • IIS Admin Service • Panda Antivirus Service • Update Services • Windows Deployment Services Server
Contdom01	• Active Directory Dmain Services • Active Directory Web Services • DNS Server • Hp Insight Server Agents • Panda Antivirus Service
dmzserver	• Autodesk MapGuide Server 6.5 • Hp Insight Server Agents • MapGuide Server 2.2 • MapGuide LightView 6.5 • Panda Antivirus Service • PostGresql Server 8.3 • Service Admin IIS • SQL Server (SQLExpress)

Tabela 3 - Serviços a serem monitorizados pelo "Nagios"

- ***Active Directory Domain Services*** – Armazena uma estrutura de dados e gere a comunicação entre os utilizadores e o domínio a que pertencem.
- ***DNS Server*** – Traduz o nome de computador para IP.
- ***File Services*** – Disponibiliza pastas para partilha de ficheiros.
- ***Internet Information Services*** – Servidor web para alojamento de página/aplicações web
- ***Dynamic Host Configuration Protocol*** – Atribui IP aos endereços MAC das placas de rede conectadas.
- ***Hp Insight Server Agents*** – Agente utilizado para a realização de backups para uma dispositivo de Tapes de backup.
  - ***MapGuide Server 2.4*** – É uma plataforma web para ser utilizada por aplicações que utilizam mapas.
  - ***Postgresql-8.4*** – Servidor de base de dados.
  - ***Hyper-V*** – Aplicação para criação de máquina virtuais.
  - ***Hyper-V Networking Management Service*** – Serviço que gere as interfaces de rede virtuais utilizadas no Hyper-V.
  - ***Autodes MapGuide Server 6.5*** – Plataforma web da autodesk para geração de mapas.
  - ***SQL Server (MSSQLSERV)*** – Servidor de base de dados SQL.
  - ***SQL SERVER (SMAES)*** – Instância do SQL.
  - ***http*** – Servidor de web.
  - ***IMAP*** – Servidor de reção de emals.
  - ***SMTP*** – Servidor de envio de emails.
  - ***Smbd*** – Servidor de partilha de ficheiros.
  - ***Sshd*** – Servidor de ligações remotas.
  - ***Mysqld*** – Servidor de base de dados MySQL.
  - ***Postgres*** – Servidor de Base de Dados.
  - ***Active Directory Certificate Services*** – Servidor de emissão de certificados digitais.
  - ***Background Intelligent Transfer Service*** – Serviço utilizado pelos updates do Windows.
  - ***Hyper-V HearBeat Service*** – Serviço que monitoriza o estado.
  - ***Microsoft Exchange Active Directory Topology*** – Servidor de Exchange da Microsoft.
  - ***Microsoft Forefront Server Protection Controller*** – Antivirus da Microsoft.
  - ***Microsoft Forefront TMG Firewall*** – Firewall da Microsoft.
  - ***Update Services*** – Serviço de updates Microsoft.

- ***Windows Deployment Services Server*** – Servidor de imagens de sistemas operativos.
- ***Panda Antivirus Service*** – Serviço de antivírus do Panda.

Para a monitorização dos serviços anteriormente mencionados é necessário instalar em cada máquina a aplicação/agente "NSClient++". Este agente basicamente permite efetuar verificações remotas e permite que o "Nagios" realize pedidos, através de comandos, para saber o estado de determinado serviço ou característica do computador.

Na Câmara Municipal só foi permitida a instalação deste agente nas seguintes máquinas, com o objetivo de efetuar a monitorização de alguns serviços:

Servidor	Serviços
2009server	• CPU Load • FTP • *Memory Usage*
Fileserver	• FTP
Exchange2010	• IMAP • SMTP
SQL	• MSSQL • *Memory Usage*

Tabela 4 - Máquinas onde se encontra instalado "NSCLient++"

O servidor "Contas2" é onde se encontra implementado o sistema documental utilizado por todos os funcionários da Câmara Municipal. É uma aplicação onde estão configurados *workflows*

para documentos tais como informações internas, férias, e outros documentos importantes que precisam de pareceres dos diferentes serviços.

Como muitos destes documentos entram na Câmara Municipal através do cidadão é importante que a disponibilidade do servidor seja algo muito importante para o bom funcionamento dos serviços.

Sendo que o sistema de monitorização "Nagios" monitoriza os serviços do "contas2" apresentados na tabela seguinte.

Servidor	Serviços
Contas2	• http • IMAP • SMTP • SSH

Tabela 5 - Serviços do Contas2 a serem monitorizados pelo Nagios

O sistema documental da "iPortalDoc" funciona essencialmente à base de envio de *emails* para notificar os seus utilizadores para a realização de uma qualquer ação sobre um documento introduzido na Gestão Documental.

5. Sistema de Monitorização na Câmara Municipal de Santo Tirso

5.1.Nagios

De tudo que foi exposto até aqui, a escolha da ferramenta pode ser uma tarefa complexa, já que a oferta é muita e as funcionalidades semelhantes. A ferramenta selecionada foi o "Nagios" dado se tratar de uma ferramenta que dispõe de uma grande variedade de funcionalidades e de interação simples.

Trata-se de uma aplicação que permite a configuração à medida da organização.

A ferramenta foi instalada num servidor com as seguintes características:

- Processador Intel Xeon 2.60GHz;
- Arquitetura i686 32-Bit;
- 3G de RAM;
- CentOS release 6.6;
- Duas placas de rede. Uma a 100Mb/s e outra a 1000Mb/s.

Após a instalação é necessário efetuar a configuração dos equipamentos para serem monitorizados pelo "Nagios".

Para uma melhor organização dos ficheiros de configuração foram criadas várias pastas relativas aos diferentes tipos de equipamentos. A figura seguinte mostra a árvore de pastas criada:

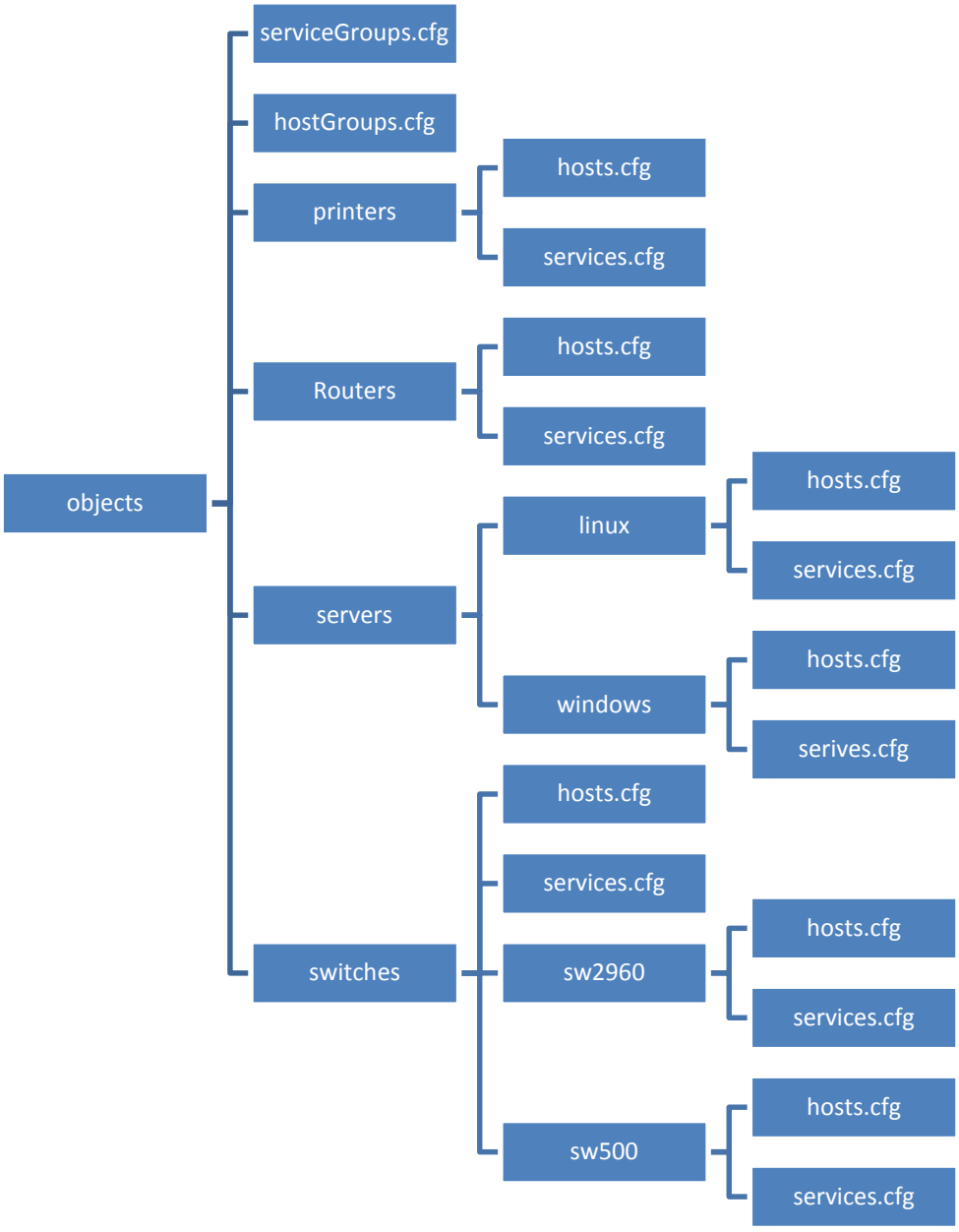


Figura 19 - Arvore dos ficheiros de configuração do "Nagios"

Para que os ficheiros de configuração sejam lidos pelo Nagios é necessário introduzir o caminho de cada ficheiro no ficheiro de configuração "Nagios.cfg":

cfg_file=/usr/local/nagios/etc/objects/commands.cfg

cfg_file=/usr/local/nagios/etc/objects/contacts.cfg

cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg

```
cfg_file=/usr/local/nagios/etc/objects/templates.cfg
cfg_file=/usr/local/nagios/etc/objects/hostGroups.cfg
cfg_file=/usr/local/nagios/etc/objects/serviceGroups.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/servers/linux/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/servers/linux/services.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/servers/windows/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/servers/windows/services.cfg

# Definitions for monitoring a router/switch
cfg_file=/usr/local/nagios/etc/objects/switches/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/switches/services.cfg

# Definitions for monitoring a router/switch
cfg_file=/usr/local/nagios/etc/objects/switches/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/switches/services.cfg

cfg_file=/usr/local/nagios/etc/objects/switches/sw2960/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/switches/sw2960/services.cfg

cfg_file=/usr/local/nagios/etc/objects/switches/sw500/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/switches/sw500/services.cfg

# Definitions for monitoring a network router
cfg_file=/usr/local/nagios/etc/objects/routers/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/routers/services.cfg

# Definitions for monitoring a network printer
cfg_file=/usr/local/nagios/etc/objects/printers/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/printers/services.cfg
```

5.1.1. Snmpwalk

"Snmpwalk" é uma aplicação utilizada para percorrer uma MIB e obter os dados dos respetivos ODI's.

Esta aplicação foi utilizada para aceder às MIB's dos equipamentos a monitorizar para obter os OID's necessários nos comandos da ferramenta "Nagios".

Os comandos necessários para obter a árvore de OID's e resultados da MIB do Switch "Informatica_4500": snmpwalk –v1 –c m1nh0ca 10.1.102.254 | more"

SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.2(25)EWA4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri 23-Sep-05 13:31 by ssearc
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.501
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (593227596) 68 days, 15:51:15.96
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: INFORMATICA_4500
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 6
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00

IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifAdminStatus.3 = INTEGER: up(1)
IF-MIB::ifAdminStatus.4 = INTEGER: up(1)
IF-MIB::ifAdminStatus.5 = INTEGER: up(1)
IF-MIB::ifAdminStatus.6 = INTEGER: up(1)
IF-MIB::ifAdminStatus.7 = INTEGER: up(1)
IF-MIB::ifAdminStatus.8 = INTEGER: up(1)
IF-MIB::ifAdminStatus.9 = INTEGER: up(1)
IF-MIB::ifAdminStatus.10 = INTEGER: up(1)
IF-MIB::ifAdminStatus.11 = INTEGER: up(1)

IF-MIB::ifOperStatus.2 = INTEGER: down(2)

IF-MIB::ifOperStatus.3 = INTEGER: down(2)

IF-MIB::ifOperStatus.4 = INTEGER: down(2)

IF-MIB::ifOperStatus.5 = INTEGER: down(2)

IF-MIB::ifOperStatus.6 = INTEGER: up(1)

IF-MIB::ifOperStatus.7 = INTEGER: up(1)

IF-MIB::ifOperStatus.8 = INTEGER: up(1)

IF-MIB::ifOperStatus.9 = INTEGER: up(1)

IF-MIB::ifOperStatus.10 = INTEGER: up(1)

IF-MIB::ifOperStatus.11 = INTEGER: up(1)

Este exemplo pode-se verificar que existe um OID para cada estado das portas. Onde ifOperStatus.6 refere-se à porta número 6 e é obtido o estado do link,

ifAdminStatus.6 refere-se à porta número 6 e é obtido o estado da porta.

Depois de selecionar os OID's a monitorizar é necessário introduzi-los nos ficheiros de configuração dos serviços no "Nagios".

5.1.2. Grupos de serviços e grupos de *hosts*

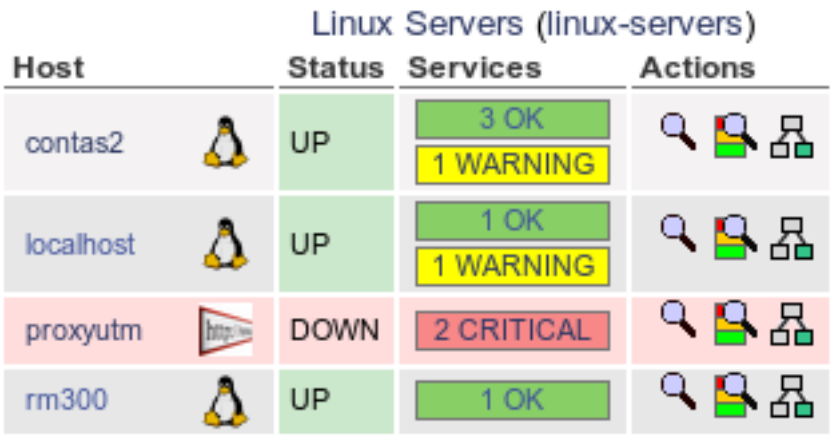
- **/usr/local/nagios/etc/objects/hostGroups.cfg**

Foi decidido agrupar os *hosts* pelo mesmo tipo de equipamento visto que muitos deles são do mesmo marca e modelo. Desta forma quando se verificam serviço é possível com o mesmo comando analisar os *hosts* desse grupo.

Windows Servers (windows-servers)

Host	Status	Services	Actions
2009server	UP	3 OK 1 CRITICAL	
ConfigMgr	UP	No matching services	
Dmzserver	UP	1 WARNING	
Fileserver	UP	1 OK	
Sigserver	UP	No matching services	
biblioteca_server	UNREACHABLE	No matching services	
contdom01	UP	No matching services	
exchange	UP	2 OK 1 WARNING	
hyperv01	UP	No matching services	
hyperv02	UP	No matching services	
scav2013	UP	No matching services	
sql	UP	1 OK 3 CRITICAL	
sql02	DOWN	No matching services	
sql03	DOWN	No matching services	
tmg01	DOWN	No matching services	

Figura 20 - *Hosts* do grupo windows-servers



Linux Servers (linux-servers)

Host	Status	Services	Actions
contas2	UP	3 OK 1 WARNING	
localhost	UP	1 OK 1 WARNING	
proxyutm	DOWN	2 CRITICAL	
rm300	UP	1 OK	

Figura 21 - *Hosts* do grupo linux-servers

Nas figuras anteriores pode-se observar as tabelas geradas pelo "Nagios" e que permitem verificar o estado dos *link* se dos serviços monitorizados nos servidores *Windows* e *Linux*.

Pode-se verificar que o "Nagios" não consegue verificar o estado do link de alguns servidores colocando o seu estado com "*DOWN*". O estado "*UNREACHABLE*" representa a situação em que o servidor pode estar ativo mas pelo facto de algum equipamento intermédio estar "*DOWN*" o "Nagios" não consegue verificar o estado do *link* nesse servidor. O Estado "*UP*" significa que o servidor se encontra ativo.

Na secção dos serviços pode-se verificar que, por exemplo no servidor 2009server, encontram-se quatro serviços a serem monitorizados, sendo que três estão em prefeito funcionamento e um se encontra em estado crítico.

Quando se verifica que um servidor se encontra no estado "*DOWN*", "*UNREACHABLE*" ou um serviço no estado critico o técnico responsável por esse servidor recebe uma notificação através de *email* com detalhes sobre o problema que está a ocorrer no servidor. Quando voltar tudo ao normal o técnico é novamente notificado com a informação que o problema se encontra resolvido.

Network Cisco Switches (switches)

Host	Status	Services	Actions
drh	UP	25 OK	
fabrica_sthyrso	UP	28 OK	
gap	UP	27 OK	
informatica_4500	UP	61 OK 6 WARNING 11 CRITICAL	
museu	UP	28 OK 1 CRITICAL	

Figura 22 - *Hosts* do grupo *switches*

Network Cisco Switches 2960 (switches_2960)

Host	Status	Services	Actions
acao-social_2960	UP	50 OK	
arquivo	UP	54 OK	
dop_2960	UP	50 OK	
dotig_2960	UP	50 OK	
tesouraria_2960	UP	50 OK	

Figura 23 - *Hosts* do grupo *switches*_2960

Network Cisco Switches 500 (switches_500)

Host	Status	Services	Actions
DOM	UP	28 OK	
ambiente	UP	28 OK	
armazem	UP	27 OK 1 CRITICAL	
central	UP	28 OK	
cpcj	DOWN	28 UNKNOWN	
depsa	UP	28 OK	
estaleiros	UP	28 OK	
informatica2	UP	27 OK 1 CRITICAL	
informatica3	UP	28 OK	
pavilhao	UP	28 OK	
piscina	UP	28 OK	

Figura 24 - *Hosts* do grupo *switches*_500

Nas figuras anteriores pode-se verificar o estado dos *links* dos *switches* e o estado dos serviços que estão a ser monitorizados pelo "Nagios".

Os *switches* foram agrupados pela marca e modelos iguais porque as MIB's são as mesmas. Desta forma com o mesmo comando pode-se verificar todos elementos que pertencem a esse grupo.

Network routers (routers)

Host	Status	Services	Actions
biblioteca_wan2	UNREACHABLE	1 UNKNOWN	
camara_biblioteca	DOWN	1 UNKNOWN	
camara_wan1	UP	No matching services	
camara_wan2	UP	No matching services	

Figura 25 - *Hosts* do grupo *routers*

No quadro anterior pode-se consultar o estado dos *links* nos routers que se encontram fisicamente na Câmara e na biblioteca. É importante monitorizar o estado dos *links* deste tipo de equipamento porque é o responsável pelas comunicações para o exterior da organização. Os técnicos responsáveis pelos *links* devem ser notificados o mais rápido possível caso ocorra algum problema nos links.

Uma forma de minimizar o impacto de uma falha de rede por parte do ISP (*Internet Service Provider*) é colocar um segundo ISP, permitindo assim haver redundância. No *link* camara_wan1 encontra-se um ISP e no camara_wan2 encontra-se um segundo ISP.

Network Printers (network-printers)

Host	Status	Services	Actions
canon_ir_1730_cpcj	UP	1 OK	
canon_ir_1730_das	UP	1 OK	
canon_ir_1730_pm	UP	1 OK	
canon_ir_2525_dag	UP	1 OK	
canon_irc_2016i_si	UP	1 OK	
canon_irc_2020i_compras	UP	1 OK	
canon_irc_2020i_drh	UP	1 OK	
canon_irc_2220_museu	DOWN	1 UNKNOWN	
canon_irc_2220_pav	UP	1 OK	
canon_irc_2880i_dop	UP	1 OK	
canon_irc_2880i_dph	UP	1 OK	
canon_irc_3080i_bu	UP	1 OK	
canon_irc_3080i_dom	UP	1 OK	
canon_irc_3580_gap	DOWN	1 UNKNOWN	
hplj2605dn	UP	1 OK	

Figura 26 - *Hosts* do grupo network-printers

Neste sistema de monitorização verificou-se ser de elevada importância a monitorização das impressoras de rede que se encontram espalhas pelo edifício na Câmara.

Pode-se verificar no quadro apresentado na figura anterior o estado dos *links* e dos serviços dessas impressoras.

- **/usr/local/nagios/etc/objects/serviceGroups.cfg**

Foi decido agrupar 3 tipos de serviços:

- A contagem do número de folhas impressas pelas multifunções;
- A largura de banda ocupada em cada porta de rede do *switch* “informática_4500”;
- O estado dos *links* e das portas de rede no *switch* “informática_4500”.

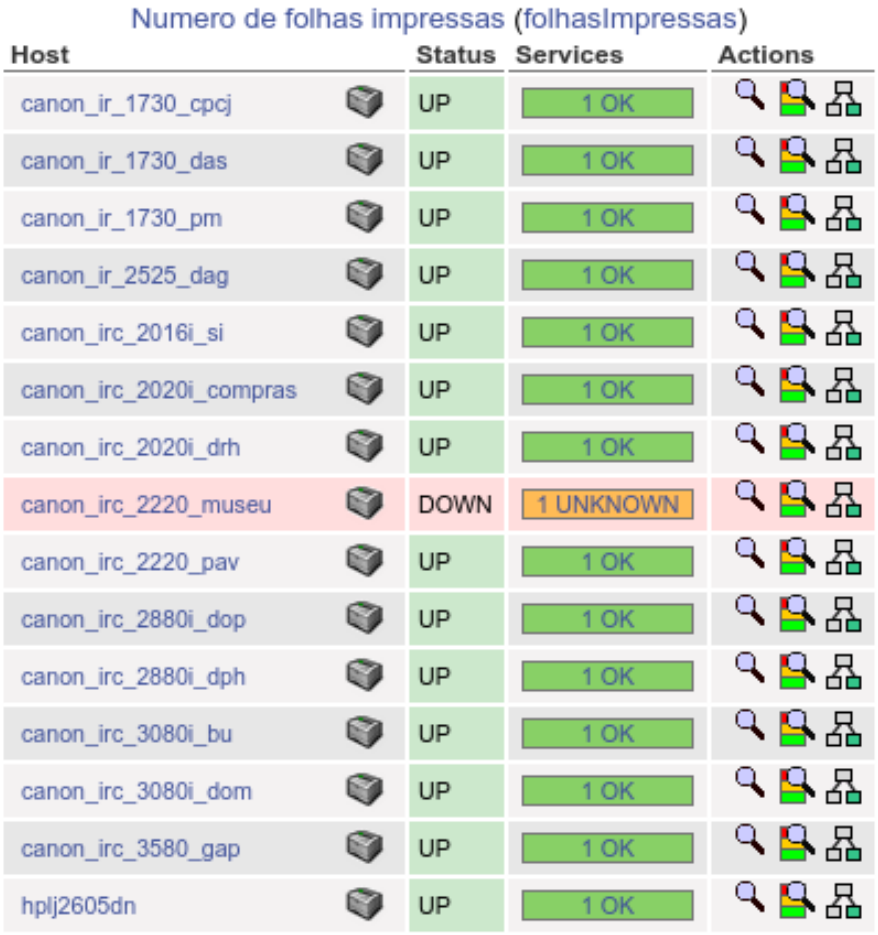


Figura 27 - Serviços do grupo folhasImpressas

O quadro anterior mostra o estado do serviço "folhasImpressas" em cada uma das impressoras de rede monitorizadas.

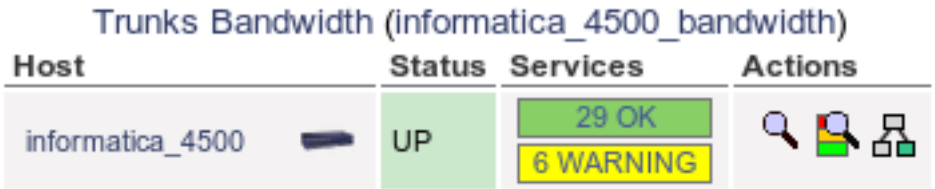


Figura 28 - Serviços do grupo informatica_4500_bandwidth

O quadro apresentado na figura anterior mostra o estado do serviço que obtém a largura de banda de cada uma das portas de rede e fibra que se encontram no *switch* "informática_4500".

Através da monitorização deste serviço os técnicos podem verificar em que *links* se encontra um maior trafego de dados.

Por vezes podem ocorrer grandes fluxos de tráfegos num único *link* fazendo com que a velocidade de transmissão de dados seja reduzida. Isto pode acontecer devido a um vírus ou um ataque DoS (*Denial of Serviçe*). Pelo que quando um *link* está com demasiado trafego é gerado um notificação pelo "Nagios" e enviada para o técnico responsável.

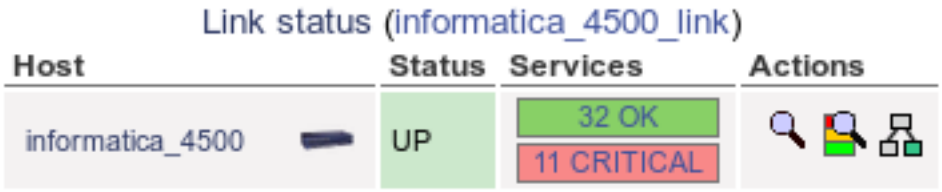


Figura 29 - Serviços do grupo informatica_4500_link

Na figura anterior pode-se observar o estado do serviço que recebe o estado de cada uma das portas de rede e fibra que se encontram no *switch* "informática_4500".

Com a monitorização deste serviço é possível obter o estado de cada uma das portas do *switch*. É possível verificar dois estados nessas portas, o estado do *link* e o estado físico da porta. O estado do *link* verifica se está a ocorrer comunicação entre aquela porta de rede e a porta de rede com que comunica, o estado físico da porta unicamente verifica se aquela porta está ativa, ou não independentemente do estado *link*.

5.1.3. Monitorização de servidores

Host	Service	Status	Last Check	Duration	Attempt
2009server	CPU Load	OK	11-21-2014 11:10:27	17d 18h 26m 16s	1/3
	FTP	OK	11-21-2014 11:11:07	17d 18h 25m 36s	1/3
	HTTP	CRITICAL	11-21-2014 11:11:57	35d 11h 4m 47s	3/3
	Memory Usage	OK	11-21-2014 11:12:37	17d 18h 25m 56s	1/3
Dmzserver	HTTP	WARNING	11-21-2014 11:03:17	41d 10h 43m 17s	3/3
Fileserver	FTP	OK	11-21-2014 11:06:07	4d 1h 47m 1s	1/3
exchange	HTTP	WARNING	11-21-2014 11:12:57	51d 12h 53m 35s	3/3
	IMAP	OK	11-21-2014 11:03:47	51d 12h 58m 45s	1/3
	SMTP	OK	11-21-2014 11:04:27	31d 23h 10m 7s	1/3
sql	CPU Load	CRITICAL	11-21-2014 11:05:27	298d 20h 48m 48s	3/3
	HTTP	OK	11-21-2014 11:06:07	19d 23h 34m 31s	1/3
	MSSQL	CRITICAL	11-21-2014 11:06:57	298d 20h 53m 48s	3/3
	Memory Usage	CRITICAL	11-21-2014 11:07:37	298d 20h 46m 38s	3/3

Figura 30 - Servidores Windows

Host	Service	Status	Last Check	Duration	Attempt
contas2	HTTP	WARNING	11-21-2014 11:10:37	13d 20h 8m 7s	3/3
	IMAP	OK	11-21-2014 11:11:27	43d 18h 45m 18s	1/3
	SMTP	OK	11-21-2014 11:12:07	43d 18h 50m 28s	1/3
	SSH	OK	11-21-2014 11:12:47	18d 7h 35m 57s	1/3
localhost	HTTP	WARNING	11-21-2014 11:10:58	400d 20h 30m 45s	3/3
	SSH	OK	11-21-2014 11:11:47	400d 20h 28m 52s	1/3
proxyutm	SMTP	CRITICAL	11-21-2014 11:13:17	227d 0h 3m 37s	3/3
	SSH	CRITICAL	11-21-2014 11:13:57	227d 0h 1m 27s	3/3
rm300	SMTP	OK	11-21-2014 11:14:47	15d 0h 39m 58s	1/3

Figura 31 - Servidores Linux

Nas figuras anteriores pode-se verificar com mais detalhe que serviços estão a ser monitorizados e em que servidor.

Para verificar serviços num servidor Windows é necessária a instalação de um agente que obtém as informações sobre o estado dos serviços e a envia para o Nagios. O agente é o “NSCliente++”.

O comando “check_nt” é utilizado para interagir com o agente “NSCliente++” instalado nos servidores *Windows*.

O comando check_smtp faz a monitorização do serviço de envio de *emails*. Esta monitorização é fundamental principalmente no servidor "contas2". Pois caso, exista uma anomalia os administradores são notificados através de um *email* enviado pelo Nagios com informação detalhada, permitindo uma rápida resolução.

5.1.4. Monitorização de *switches*

- **/usr/local/nagios/etc/objects/switches/hosts.cfg**

Pode-se constatar pela definição do *host* anterior, "informática_4500", que quando esta verificação não é bem-sucedida o Nagios envia uma notificação aos contactos dos grupos admins e carneiroAdmin. Esta verificação é realizada em períodos de 120 minutos.

Neste ficheiro de *hosts* estão configurados os *switches* GAP, informática_4500, museu; drh e fabrica_sthyriso.

- **/usr/local/nagios/etc/objects/switches/services.cfg**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
informatica_4500	Port G03/01 PAVILHÃO Bandwidth Usage	OK	11-20-2014 17:28:07	9d 2h 40m 0s	1/3	Traffic OK - Max. In = 9.6 KB/s, Max. Out = 18.3 KB/s
	Port G03/02 DOM Bandwidth Usage	OK	11-20-2014 17:29:37	10d 2h 55m 0s	1/3	Traffic OK - Max. In = 37.0 KB/s, Max. Out = 102.1 KB/s
	Port G03/03 DRH Bandwidth Usage	OK	11-20-2014 17:30:57	10d 2h 51m 26s	1/3	Traffic OK - Max. In = 22.7 KB/s, Max. Out = 139.7 KB/s
	Port G03/04 DOTIG Bandwidth Usage	OK	11-20-2014 17:32:27	9d 1h 19m 56s	1/3	Traffic OK - Max. In = 17.9 KB/s, Max. Out = 102.5 KB/s
	Port G03/05 DEPSA Bandwidth Usage	OK	11-20-2014 17:33:47	9d 1h 29m 53s	1/3	Traffic OK - Max. In = 24.2 KB/s, Max. Out = 130.1 KB/s
	Port G03/06 ARQUIVO Bandwidth Usage	OK	11-20-2014 17:25:23	9d 1h 29m 53s	1/3	Traffic OK - Max. In = 12.0 KB/s, Max. Out = 21.6 KB/s
	Port G04/01 TESOURARIA Bandwidth Usage	OK	11-20-2014 17:26:47	9d 1h 29m 26s	1/3	Traffic OK - Max. In = 51.8 KB/s, Max. Out = 103.8 KB/s
	Port G04/02 DOPSA Bandwidth Usage	OK	11-20-2014 17:28:07	9d 2h 39m 59s	1/3	Traffic OK - Max. In = 6.0 KB/s, Max. Out = 13.9 KB/s
	Port G04/03 ARMAZEM Bandwidth Usage	OK	11-20-2014 17:29:37	10d 2h 55m 1s	1/3	Traffic OK - Max. In = 310.0 KB/s, Max. Out = 48.6 KB/s
	Port G04/04 AMBIENTE Bandwidth Usage	WARNING	11-20-2014 17:30:57	9d 1h 26m 41s	3/3	MRTG data has expired (14685 minutes old)
	Port G04/05 ESTALEIROS Bandwidth Usage	OK	11-20-2014 17:32:27	9d 1h 19m 56s	1/3	Traffic OK - Max. In = 1.3 KB/s, Max. Out = 4.8 KB/s
	Port G04/06 MUSEU Bandwidth Usage	OK	11-20-2014 17:33:47	9d 1h 29m 53s	1/3	Traffic OK - Max. In = 12.7 KB/s, Max. Out = 69.1 KB/s
	Port G05/02 EXCHANGE Link 1 Bandwidth Usage	WARNING	11-20-2014 17:26:07	9d 1h 33m 52s	3/3	MRTG data has expired (14681 minutes old)
	Port G05/04 2009SERVER Bandwidth Usage	OK	11-20-2014 17:28:17	9d 2h 39m 58s	1/3	Traffic OK - Max. In = 42.8 KB/s, Max. Out = 69.9 KB/s
	Port G05/05 SIGSERVER Link 1 Bandwidth Usage	OK	11-20-2014 17:29:37	10d 2h 55m 1s	1/3	Traffic OK - Max. In = 9.0 B/s, Max. Out = 4.2 KB/s
	Port G05/06 SIGSERVER Link 2 Bandwidth Usage	OK	11-20-2014 17:30:57	10d 2h 51m 36s	1/3	Traffic OK - Max. In = 73.4 KB/s, Max. Out = 438.1 KB/s
	Port G05/08 CONTDOM01 Link 1 Bandwidth Usage	WARNING	11-20-2014 17:33:07	9d 1h 33m 56s	3/3	MRTG data has expired (14688 minutes old)
	Port G05/09 FOG Bandwidth Usage	OK	11-20-2014 17:34:37	9d 1h 29m 53s	1/3	Traffic OK - Max. In = 53.5 KB/s, Max. Out = 3.4 KB/s
	Port G05/11 Bandwidth Usage	OK	11-20-2014 17:26:47	9d 1h 29m 24s	1/3	Traffic OK - Max. In = 12.0 B/s, Max. Out = 24.2 KB/s
	Port G05/12 FILESERVER Link 1 Bandwidth Usage	WARNING	11-20-2014 17:28:17	9d 1h 31m 57s	3/3	MRTG data has expired (14683 minutes old)
	Port G05/13 HYPERV01 Bandwidth Usage	OK	11-20-2014 17:29:37	10d 2h 54m 59s	1/3	Traffic OK - Max. In = 32.9 KB/s, Max. Out = 4.2 KB/s
	Port G05/14 NAGIOSSERVER Bandwidth Usage	OK	11-20-2014 17:30:57	10d 2h 51m 26s	1/3	Traffic OK - Max. In = 6.0 B/s, Max. Out = 3.4 KB/s
	Port G05/15 SQL Link 1 Bandwidth Usage	OK	11-20-2014 17:32:27	10d 2h 51m 26s	1/3	Traffic OK - Max. In = 54.8 KB/s, Max. Out = 3.2 KB/s
	Port G05/16 FILESERVER Link 2 Bandwidth Usage	OK	11-20-2014 17:33:57	9d 1h 19m 53s	1/3	Traffic OK - Max. In = 14.0 B/s, Max. Out = 3.3 KB/s
	Port G05/17 CONTAS2 Bandwidth Usage	OK	11-20-2014 17:25:23	9d 1h 19m 53s	1/3	Traffic OK - Max. In = 1.2 KB/s, Max. Out = 4.2 KB/s
	Port G05/18 NA Bandwidth Usage	OK	11-20-2014 17:26:47	9d 1h 29m 23s	1/3	Traffic OK - Max. In = 1.0 KB/s, Max. Out = 4.3 KB/s
	Port G05/19 SQL Link 2 Bandwidth Usage	OK	11-20-2014 17:28:17	9d 2h 39m 57s	1/3	Traffic OK - Max. In = 271.0 KB/s, Max. Out = 79.4 KB/s
	Port G05/20 HYPERV01 Bandwidth Usage	OK	11-20-2014 17:29:37	10d 2h 55m 1s	1/3	Traffic OK - Max. In = 84.0 B/s, Max. Out = 4.6 KB/s
	Port G05/21 EXCHANGE Link 2 Bandwidth Usage	OK	11-20-2014 17:30:57	9d 1h 28m 56s	1/3	Traffic OK - Max. In = 1.7 KB/s, Max. Out = 4.4 KB/s
	Port G05/22 INFORMATICA3 Bandwidth Usage	OK	11-20-2014 17:32:27	9d 1h 19m 56s	1/3	Traffic OK - Max. In = 1.2 KB/s, Max. Out = 5.6 KB/s
	Port G05/23 INFORMATICA2 Bandwidth Usage	WARNING	11-20-2014 17:33:57	9d 1h 33m 53s	3/3	MRTG data has expired (14688 minutes old)
	Port G05/24 BACKUPS Bandwidth Usage	WARNING	11-20-2014 17:25:23	9d 1h 33m 52s	3/3	MRTG data has expired (14680 minutes old)
	Port Vlan01_172.16.10.101_10.1.102.254_192.168.10.252 Bandwidth Usage	OK	11-20-2014 17:27:27	9d 2h 40m 39s	1/3	Traffic OK - Max. In = 66.5 KB/s, Max. Out = 66.3 KB/s
	Port Vlan04_192.168.12.254 Bandwidth Usage	OK	11-20-2014 17:28:17	9d 2h 39m 56s	1/3	Traffic OK - Max. In = 0.0 B/s, Max. Out = 4.0 B/s
	Port Vlan06_192.168.0.254 Bandwidth Usage	OK	11-20-2014 17:29:37	10d 2h 54m 59s	1/3	Traffic OK - Max. In = 0.0 B/s, Max. Out = 0.0 B/s

Figura 32 - Largura de banda nas portas do informatica_4500

Neste ficheiro de configuração está configurada a monitorização de todas as portas dos cinco *switches*, anteriores mencionados. Foi decidido configurar os serviços dos *switches* no mesmo ficheiro pelo facto de apenas serem cinco. No entanto, deveria ser adotado ficheiro de configuração de serviços para cada um dos *switches*.

Como se pode verificar no exemplo de configuração dos serviços pode-se concluir que são efetuadas duas verificações por porta. "check_snmp!-C m1nh0ca -o ifOperStatus.23 -r 1 -m RFC1213-MIB" verifica o estado em que se encontra a porta, isto é, se ela esta com link ativo, ou não.

Normalmente é utilizado nos *links* entre *swithces* "check_local_mrtgtraf!/var/www/mrtg/informatica_4500/10.1.102.254_23.log!MAX!102400000,102400000!121600000,121600000!10" através deste comando o Nagios verifica a largura máxima utiliza num determinado momento, normalmente de 5 em 5 minutos faz esta verificação.

Caso seja uma porta de acesso ao *switch* é necessário utilizar o seguinte comando: "check_snmp!-C m1nh0ca -o ifAdminStatus.23 -r 1 -m RFC1213-MIB". Com este comando só é verificado o estado da porta, isto é se está operacional, ou não. Não necessita que esteja algum dispositivo conectado, caso contrário sempre que alguém desligasse um computador seria enviado para o administrador uma notificação que o *link* estava com problemas.

Todos os ficheiros de configuração dos *hosts* e serviços dos vários *swithes* seguem o exemplo anterior.

5.1.5. Monitorização de impressoras

- **/usr/local/nagios/etc/objects/printers/hosts.cfg**
- **/usr/local/nagios/etc/objects/printers/services.cfg**

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
canon_ir_1730_cpcj	Folhas impressas	OK	11-20-2014 17:36:37	0d 8h 20m 28s	1/3	SNMP OK - Numero de folhas impressas - 37557 folhas
canon_ir_1730_das	Folhas impressas	OK	11-20-2014 17:35:19	0d 8h 21m 48s	1/3	SNMP OK - Numero de folhas impressas - 48108 folhas
canon_ir_1730_pm	Folhas impressas	OK	11-20-2014 17:32:08	0d 2h 4m 57s	1/3	SNMP OK - Numero de folhas impressas - 44635 folhas
canon_ir_2525_dag	Folhas impressas	OK	11-20-2014 17:28:47	0d 8h 58m 18s	1/3	SNMP OK - Numero de folhas impressas - 42540 folhas
canon_irc_2016i_si	Folhas impressas	OK	11-20-2014 17:33:27	2d 2h 3m 35s	1/3	SNMP OK - Numero de folhas impressas - 108133 folhas
canon_irc_2020i_compras	Folhas impressas	OK	11-20-2014 17:36:17	1d 6h 10m 48s	1/3	SNMP OK - Numero de folhas impressas - 128207 folhas
canon_irc_2020i_drh	Folhas impressas	OK	11-20-2014 17:34:57	36d 7h 31m 54s	1/3	SNMP OK - Numero de folhas impressas - 330255 folhas
canon_irc_2220_museu	Folhas impressas	UNKNOWN	11-20-2014 17:31:37	0d 0h 47m 28s	3/3	External command error: Timeout: No Response from 10.1.101.73:161.
canon_irc_2220_pav	Folhas impressas	OK	11-20-2014 17:36:27	0d 8h 30m 38s	1/3	SNMP OK - Numero de folhas impressas - 31643 folhas
canon_irc_2880i_dop	Folhas impressas	OK	11-20-2014 17:31:07	0d 7h 35m 58s	1/3	SNMP OK - Numero de folhas impressas - 330168 folhas
canon_irc_2880i_dph	Folhas impressas	OK	11-20-2014 17:29:56	5d 20h 27m 9s	1/3	SNMP OK - Numero de folhas impressas - 193562 folhas
canon_irc_3080i_bu	Folhas impressas	OK	11-20-2014 17:35:37	0d 8h 31m 28s	1/3	SNMP OK - Numero de folhas impressas - 188163 folhas
canon_irc_3080i_dom	Folhas impressas	OK	11-20-2014 17:31:17	6d 11h 45m 48s	1/3	SNMP OK - Numero de folhas impressas - 341931 folhas
canon_irc_3580_gap	Folhas impressas	OK	11-20-2014 17:35:28	0d 0h 11m 38s	1/3	SNMP OK - Numero de folhas impressas - 636190 folhas
hplj2605dn	Folhas impressas	OK	11-20-2014 17:35:28	6d 1h 1m 34s	1/3	SNMP OK - Numero de folhas impressas - 6986 folhas

Figura 33 - Contagem das folhas impressas

Foi realizada uma pesquisa com a ferramenta “snmpwalk”, aos OID’s das MIB’s das multifunções para saber quais correspondiam aos níveis de tinta e à contagem das folhas impressas.

5.1.6. PNP4nagios

“PNP4nagios” é um *addon* para o “Nagios”. Este *addon* tem como função analisar os dados obtidos pelos *plugins* do “Nagios” e armazená-los numa RRD-database (*Round Robin Database*). (PNP4nagios, 2013). O “PNP4nagios” tem tipos de configuração na sua instalação.

- ***Synchronous Mode***

  Esta configuração é a mais simples de integrar os dados recolhidos no coletor *process_perfdata.pl.* Cada evento ocorrido vai despoletar a execução do *process-service-perfdata* (Nagios.cfg).

- ***Bulk Mode***

  Esta configuração é mais complexa do que a anterior, no entanto, reduz significativamente a carga no “Nagios” porque o coletor de dados *process_perfdata.pl* não é invocado sempre que existe um comando de monitorização de serviço. Esta configuração coloca os dados, temporariamente, num ficheiro e este é processado pelo *process_perfdata.pl* em intervalos de tempo. O Nagios fica encarregue de executar esse processo periodicamente.

- ***Bulk Mode with NPCD***

  A única diferença desta configuração com a anterior é o camando que é executado. Com este comando o ficheiro *servisse-perfdata* é movido para a pasta var/spool/ depois de um intervalo de

tempo configurado no *service_perfdata_file_processing_interval.* A macro $TIMET$ do Nagios é adicionada ao nome do ficheiro para que não haja substituição de ficheiros. Estes ficheiros são guardados na pasta /usr/local/pnp4nagios/var/spool/ para depois serem processados pelo NPCD. O NPCD monitoriza esta pasta e transfere os ficheiro para o *process_perfdata.pl.* Desta forma o processamento dos dados é completamente independente do "Nagios".

- ***Bulk Mode with NPCD and npcdmod***

Esta configuração utiliza um *broker module npcdmod.o*

- ***Gearman Mode***

Utilizada para grandes implementações de monitorização utilizando o "Nagios". Desta forma é possível utilizar o "Nagios" e o "PNP4nagios" em máquinas diferentes.

Na Câmara Municipal de Santo Tirso decidiu-se implementar o "PNP4nagios" no modo de configuração *Bulk Mode With NPCD*.

Como o computador onde se encontra o "Nagios" é um computador com pouca memória concluiu-se que este modo seria o mais indicado porque o processamento dos dados não seria feito pelo "Nagios" mas sim pelo NPCD. Assim, consegue-se manter o desempenho necessário para o bom funcionamento das monitorizações a serem realizadas.

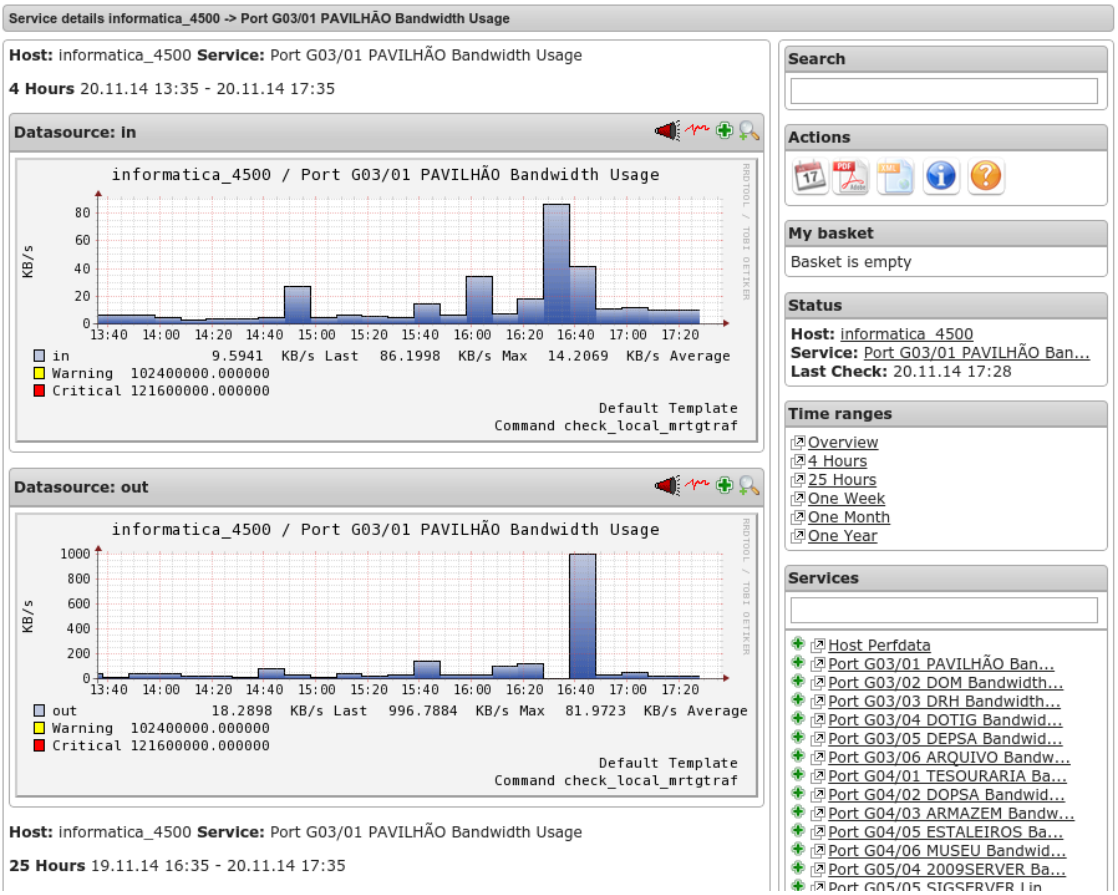


Figura 34 - PNP4nagios no *switch* informatica_4500

Da observação da figura anterior verifica-se que o comando utilizado para a monitorização da largura de banda foi "check_local_mrtgraf". Como o switch informática_4500 é o *core* na rede estruturada da Câmara é muito importante monitorizar a largura de banda ocupada pelos *links* com outros *switches*.

Foi instalado e configurado o *plugin* "MRTG" para ser utilizado juntamente com o "Nagios" e o "PNP4nagios" mas este *plugin* também gera os seus próprios gráficos.

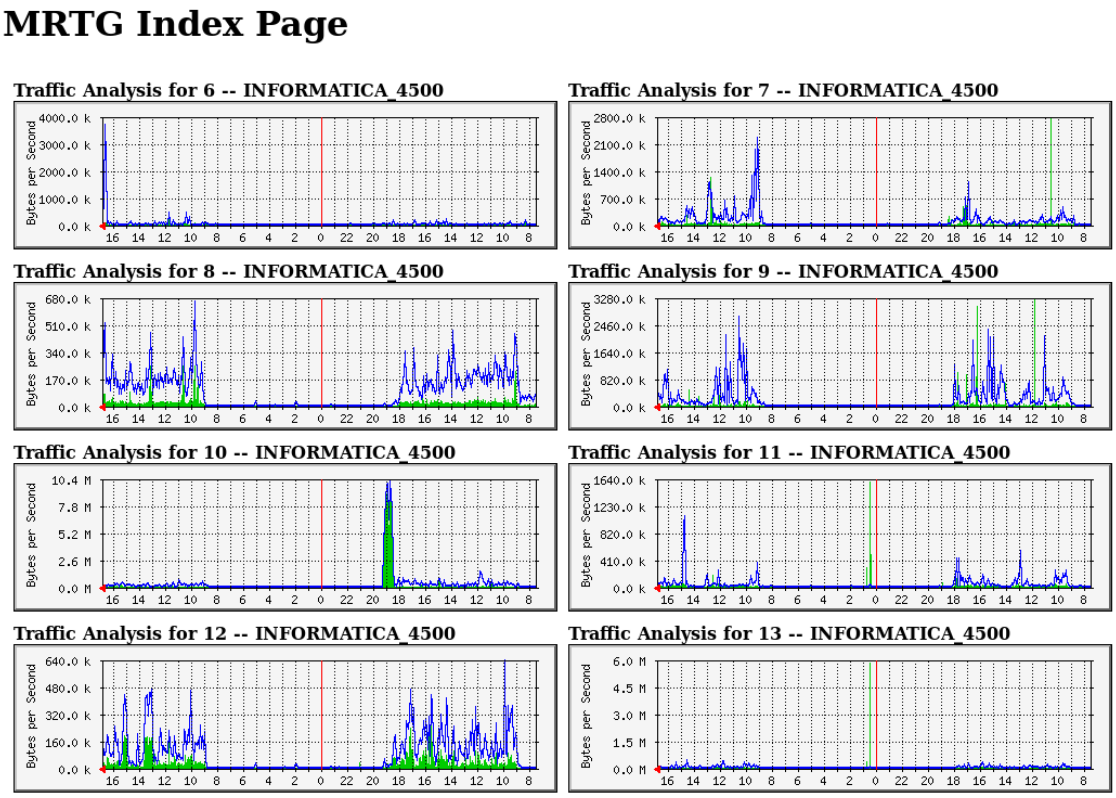


Figura 35 - MRTG (parte 1)

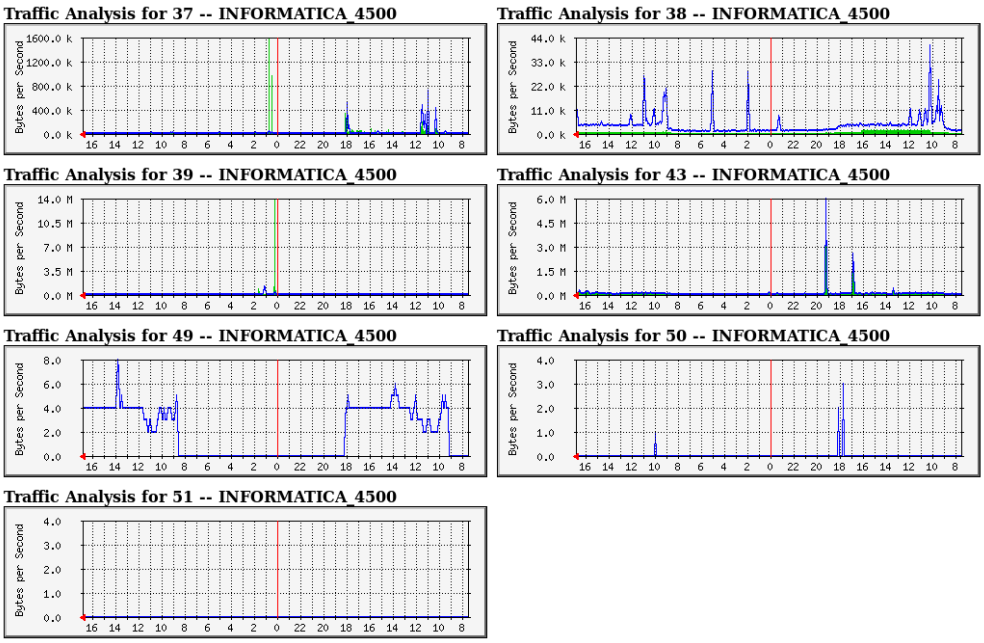


Figura 36 - MRTG (parte 2)

Nas figuras anteriores podemos analisar a largura de banda ocupada em cada interface do *switch* "informática_4500". Pode-se verificar que, sendo todas as *interfaces* a 1Gb/s, elas estão com muito pouco tráfego. A única interface que atingiu os 10Mb/s foi a *interface* número 10.

5.2.NTOPNG

Com um grande aumento de computadores e servidores na rede da Câmara Municipal de Santo tirso tornou-se essencial a utilização de uma aplicação para fazer a monitorização dos protocolos que circulam na rede de dados.

Sendo assim optou-se por utilizar a aplicação "NTOPNG". Esta aplicação encontra-se instalada no mesmo servidor do "Nagios" e utiliza a segunda placa de rede em modo promiscuo para capturar todos os pacotes que por ela passam.

A melhor forma para "copiar" todos os pacotes que circulam na rede para esta placa de rede foi conectá-la diretamente ao *switch* "informática_4500" e configurar a interface conectada em modo *span* (*Switched Port Analyzer*).

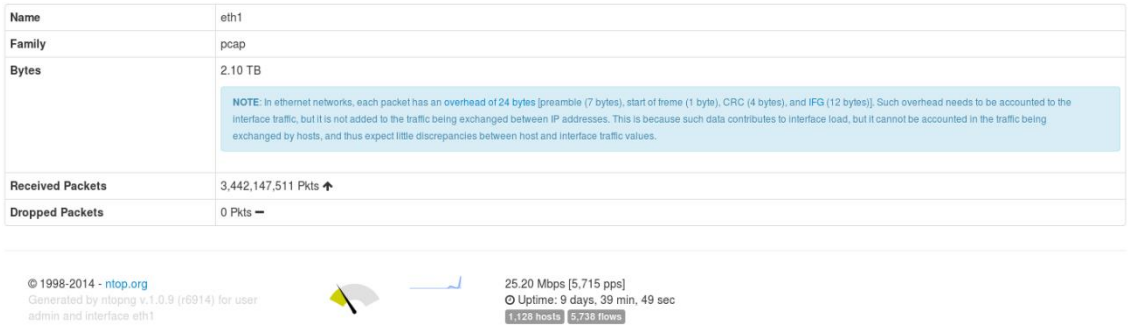


Figura 37 - NTOPNG eth1 em modo de captura

Na figura anterior pode-se verificar que ao fim de nove dias de capturas todos os pacotes que passaram pela interface eth1 foram analisados. Esta taxa de sucesso de 100% só é possível, numa máquina com limitações de *hardware*, configurando o módulo "PF_RING".

Para utilizar este módulo basta carregá-lo no *kernel* do Linux.

Na Câmara verificou-se, como esperado, que as máquinas com mais atividade nas comunicações de dados são os servidores "fileserver", "exchange2010" e "sql".

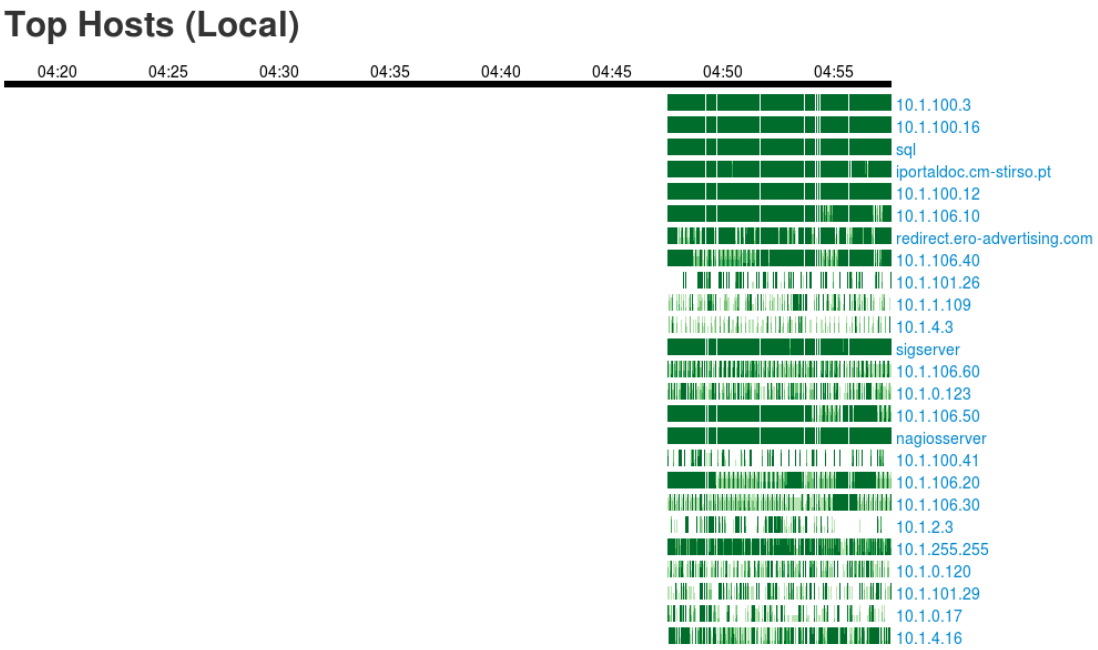


Figura 38 - Máquinas com mais atividade na rede

O servidor "fileserver – 10.1.100.3" está no topo da lista porque é o DNS primário, controlador de domínio e possui várias pastas partilhas com os utilizadores de domínio.

Segue-se o servidor de *emails* e o sql que possui as aplicações mais utilizadas na Câmara. As aplicações da medidata.

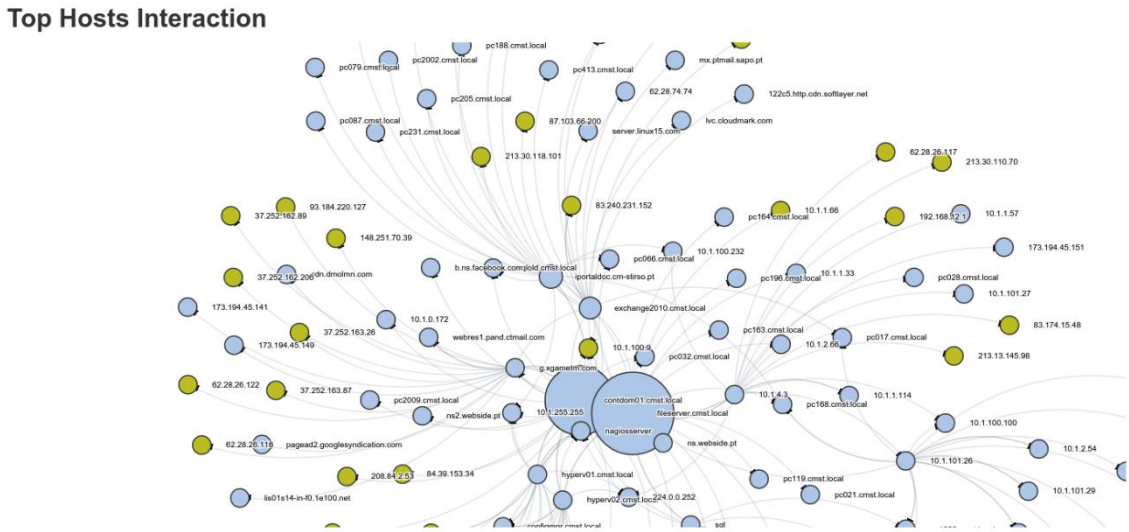


Figura 39 - Interação entre máquinas

Nesta figura consegue-se compreender a quantidade de ligações entre máquinas na intranet e máquinas na internet. Isto mostra a complexidade desta infraestrutura de dados e a crescente necessidade de sistemas de monitorização e de proteção.

Com o "NTOPNG" é possível analisar os protocolos e aplicações (*DHCP*, *DNS*, *Facebook*, *youtube*, *VPN*, entre outros) que estão a ser utilizados, em cada momento, na rede.

Com estas informações é possível verificar se existe algum tipo de ataque na rede que esteja a provocar uma subida repentina e constante de utilização da largura de banda e quem esta a provar essa anomalia. Desta forma os administradores e técnicos podem detetar e solucionar problemas graves que ocorram na rede.

5.3.OCS-Inventory

Ao longo dos anos a Câmara Municipal de Santo Tirso foi adquirindo computadores para satisfazer as necessidades dos seus colaboradores. Nos dias de hoje, praticamente todos os funcionários que trabalham nos vários serviços possuem um computador.

Este crescente número de computadores no domínio fez com que houvesse a necessidade de inventariar todos estes equipamentos. Mas, este inventário teria de ser dinâmico porque os computadores ao longo do tempo avariam, necessitam de novas peças, novos *softwares* etc.

A solução encontrada para este problema foi a implementação da aplicação web "OCS-Inventory ". Esta aplicação web é constituída por quatro componentes:

- Servidor de base de dados – Armazena a informação dos inventários;
- Servidor de comunicação – Trata das comunicações http entre o agente e a base de dados;
- Consola de administração – Permite ao administrador consultar a base de dados utilizando o *browser*;
- Servidor de distribuição - Armazena os pacotes de instalação de *software*.

Esta aplicação necessita que em cada computador seja instalado um agente. Ele é responsável por recolher os dados do computador.

5.3.1. Agente

Existem agentes para *Windows*, *Linux*, *MacOS X* e *Android*. Quando o agente é executado no computador ele comunica com o *Communication Server* utilizando o protocolo http ou https. Se o servidor não disser nada o agente não faz nada, por outro lado, o servidor pode pedir três coisas:

- Enviar um inventário: O agente envia todas as propriedades do computador utilizando o protocolo http/https. A periocidade deste inventário é configurável (OCS Windows Agent, 2013);
- Realizar um scan à rede: O agente realiza um *scanner* à rede para descobrir os dispositivos que nela se encontram. Envia esta informação por http/https para o servidor. (OCS Windows Agent, 2013);

- Instala um pacote: O agente contacta o Servidor de distribuição por https para obter um ficheiro de informação. Faz o *download* do pacote do servidor e instala-o. (OCS Windows Agent, 2013).

Numa organização com a dimensão e diversidade aqui apresentada foi necessário pensar numa solução para fazer a instalação e execução remota do agente. Para tal, no domínio foi criada uma política de grupo para todos os computadores no domínio. Quando qualquer utilizador inicia a sua sessão é instalado (caso ainda não esteja instalado) e executado o agente.

5.3.2. Consola de administração

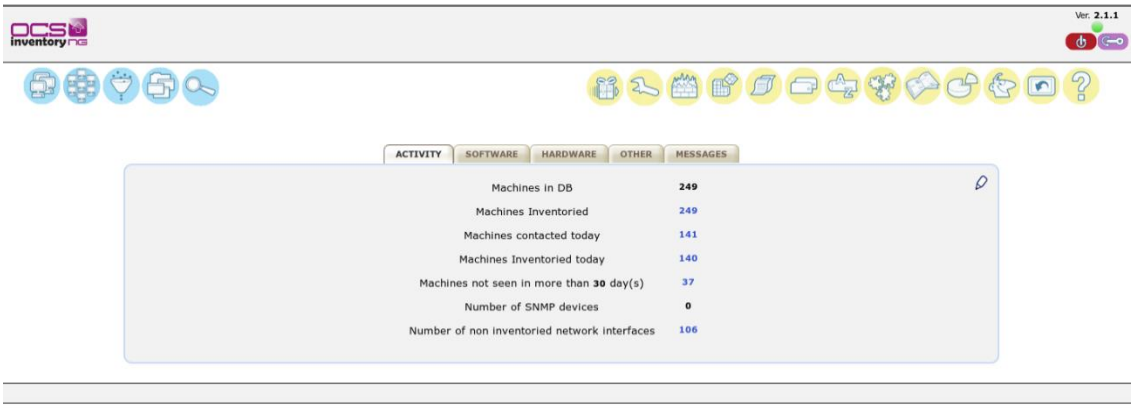


Figura 40 – OCS-Inventory

A figura anterior mostra como é apresentada a consola de administração do ocs na Câmara.

Pode-se verificar que existem duzentos e quarenta e nove computadores inventariados. Pelo que para se ter uma boa organização foi necessário criar grupos de computadores, de acordo com a sua localização.

Name	DESCRIPTION	CREATE	NBRE	Delete
BIBLIOTECA	Biblioteca	2013-11-14 12:44:20	22	
BU	Balcão Único	2013-11-14 12:45:05	8	
CCD	Centro Cultural e Desportivo	2013-11-14 12:45:33	3	
CEAN	Contratos, Expropriações e apoio ao notariado	2013-11-14 12:46:07	1	
COEF	Contra-Ordenações e Execuções Fiscais	2013-11-14 12:47:16	4	
COMPRAS	COMPRAS	2013-11-14 12:49:24	6	
CT	Central de Transportes	2013-11-14 12:49:56		
DA	Divisão de Ambiente	2013-11-14 12:50:24	8	
DAS	Divisão de Ação Social	2013-11-14 12:51:07	21	
DE	Divisão de Educação	2013-11-14 12:51:35	6	
DE(DOM)	Divisão de Empreitadas - DOM	2013-11-14 13:05:52	10	
DFC	Divisão de Finanças e Compras	2013-11-14 12:54:00	6	
DJAG	Divisão Jurídica e Administração Geral	2013-11-14 12:54:40	6	
DOM	Departamento de Obras Municipais	2013-11-14 12:55:10	7	
DOP	Divisão de Obras Particulares	2013-11-14 12:55:50	14	
DPA	Departamento de Planeamento e Ambiente	2013-11-14 12:56:24	2	
DPP	Divisão de Planeamento e projectos	2013-11-14 12:56:49	14	
DRH	Divisão de Recursos Humanos	2013-11-14 12:57:22	7	
DSG	Divisão de Serviços Gerais - DOM	2013-11-14 12:58:02	8	
DSU	Divisão de Serviços Urbanos - DOM	2013-11-14 12:58:31	1	
EGAR	Expediente Geral, Arquivo e Reprografia	2013-11-14 12:59:00	6	
FISCALIZACAO	FISCALIZACAO - DOP	2013-11-14 12:59:24	4	
GAP	Gabinete de apoio à Presidência	2013-11-14 12:59:50	9	
GAV	Gabinete de apoio à Vereação	2013-11-14 13:00:11	2	
GEFP	Gabinete de Emprego e Formação Profissional	2014-02-24 15:50:00	1	
GS	Gestão de stocks	2013-11-14 13:00:42	2	
MUSEU	MUSEU	2013-11-14 13:01:01	3	
PAVILHAO	Pavilhão e Piscina	2013-11-19 14:48:13	8	
PM	Policia Municipal	2013-11-19 14:39:43	5	
SAMA	Serviço de atendimento, Modernização administrativa	2013-11-19 14:54:39	2	
SC	Serviço de comunicação	2013-11-14 13:29:06	3	
SERVIDORES	SERVIDORES	2013-12-16 14:47:25	2	
SI	Serviço de Informática	2013-11-14 13:27:30	9	
SMAES	Serviços Municipalizados de Águas e Saniamento	2013-11-19 15:08:26	13	
ST	Serviço de Trânsito	2013-11-14 13:28:22	3	
TURISMO	TURISMO	2013-12-02 09:22:22	6	
VEREADORES	Vereadores da Câmara Municipal de Santo Tirso	2013-11-18 09:21:35	2	

Figura 41 – OCS-Inventory grupos

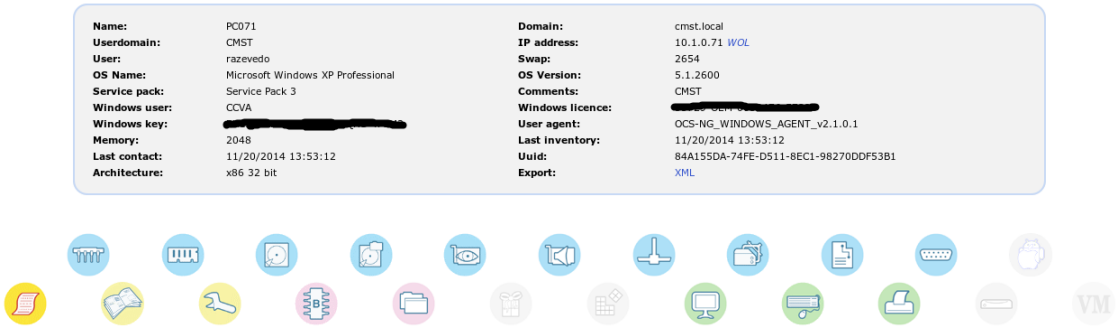
Existem trinta e sete grupos sendo o maior com vinte e dois computadores, o da biblioteca.

Esta aplicação mostrou-se muito útil para os administrador de rede porque através dela foi possível consultar os detalhes e dados muito importantes, de cada um dos computadores inventariados.

Na prática, sem sair do local de trabalho e numa função de *HelpDesk*, o técnico pode obter informação do computador do colaborador que necessita de ajuda.

Para ilustrar segue-se um exemplo:

É um facto que o parque informático da Câmara encontra-se obsoleto e com grandes défices de performance. “Um colaborador telefona a um técnico a pedir ajuda porque o seu computador está demasiado lento. O técnico acede à consola de administração do “OCS-Inventory” e procura pelo nome do computador/utilizador e logo de seguida são apresentados dados importantes sobre esse computador e sobre o *software* instalado.”



Name:	PC071	**Domain:**	cmst.local
Userdomain:	CMST	**IP address:**	10.1.0.71 *WOL*
User:	razevedo	**Swap:**	2654
OS Name:	Microsoft Windows XP Professional	**OS Version:**	5.1.2600
Service pack:	Service Pack 3	**Comments:**	CMST
Windows user:	CCVA	**Windows licence:**	[redacted]
Windows key:	[redacted]	**User agent:**	OCS-NG_WINDOWS_AGENT_v2.1.0.1
Memory:	2048	**Last inventory:**	11/20/2014 13:53:12
Last contact:	11/20/2014 13:53:12	**Uuid:**	84A155DA-74FE-D511-8EC1-98270DDF53B1
Architecture:	x86 32 bit	**Export:**	XML

Figura 42 - Inventario de um computador (parte 1)

No exemplo ilustrado na figura anterior, relativamente ao pc071 pode-se verificar que o computador ainda tem o sistema operativo *Windows xp profissional*, 2Gb de memória e um processador de 32-bits.

MEMORY

4 Result(s) (Download)

Caption	Description	Capacity (MB)	Purpose	Type	Speed	Slot number	Serial number
System Memory	BANK0 (No ECC)	2048	System Memory	SDRAM	0	1	SerNum0
System Memory	BANK1 (No ECC)	0	System Memory	Unknown	0	2	
System Memory	BANK2 (No ECC)	0	System Memory	Unknown	0	3	
System Memory	BANK3 (No ECC)	0	System Memory	Unknown	0	4	

STORAGE

3 Result(s) (Download)

Name	Manufacturer	Model	Description	Type	Disk size (MB)	Serial number	Firmware
Unidade de disquetes	(Unidades de disquete padrão)	Unidade de disquetes	Unidade de disquetes		0		
ST380011AS	(Unidades de disco padrão)	//./PHYSICALDRIVE0	Unidade	Fixed hard disk media	76316	4MR158NV	3.00
TSSTcorp CD/DVDW SH-S182M	(Unidades de CD-ROM padrão)	TSSTcorp CD/DVDW SH-S182M	Unidade de CD-ROM	CD-ROM	0		

DISK(S)

3 Result(s) (Download)

Letter	Type	Designation	File System	Free (MB)	Total (MB)	Capacity
A:	Removable Drive			0	0	
C:	Hard Drive		NTFS	24642	49999	51%
D:	CD-Rom Drive			0	0	

Figura 43 - Inventario de um computador (parte 2)

É possível obter mais detalhes, tais como quantos discos tem e qual a sua ocupação, unidades de armazenamento e se existe a possibilidade de acrescentar mais memória.

Para além das características do computador pode-se também consultar o *software* instalado.

Microsoft Corporation	Security Update for Microsoft .NET Framework 3.5 SP1 (KB2736416)	1	This security update is for Microsoft .NET Framework 3.5 SP1. If you later install a more recent service pack, this security update will be uninstalled automatically. For more information, visit http://support.microsoft.com/kb/2736416.
Microsoft Corporation	Security Update for Microsoft .NET Framework 3.5 SP1 (KB2840629)	1	This security update is for Microsoft .NET Framework 3.5 SP1. If you later install a more recent service pack, this security update will be uninstalled automatically. For more information, visit http://support.microsoft.com/kb/2840629.
Microsoft Corporation	Security Update for Microsoft .NET Framework 3.5 SP1 (KB2861697)	1	This security update is for Microsoft .NET Framework 3.5 SP1. If you later install a more recent service pack, this security update will be uninstalled automatically. For more information, visit http://support.microsoft.com/kb/2861697.
Microsoft Corporation	Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595)	1	This hotfix is for Microsoft .NET Framework 3.5 SP1. If you later install a more recent service pack, this hotfix will be uninstalled automatically. For more information, visit http://support.microsoft.com/kb/953595.
Microsoft Corporation	Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)	1	This hotfix is for Microsoft .NET Framework 3.5 SP1. If you later install a more recent service pack, this hotfix will be uninstalled automatically. For more information, visit http://support.microsoft.com/kb/958484.
Microsoft Corporation	Update for Microsoft .NET Framework 3.5 SP1 (KB963707)	1	This update is for Microsoft .NET Framework 3.5 SP1. If you later install a more recent service pack, this update will be uninstalled automatically. For more information, visit http://support.microsoft.com/kb/963707.
Medidata.Net	Preform 6.8.7	6.8.7	
GlavSoft LLC.	TightVNC	2.7.10.0	
ATI	CCC Help Danish	2009.0303.2223.40202	
ATI	Catalyst Control Center Localization All	2009.0303.2224.40202	
ATI	Skins	2009.0303.2224.40202	
ATI	Catalyst Control Center Core Implementation	2009.0303.2224.40202	
Panda Security	Panda Endpoint Agent	7.00.00.0000	
Analog Devices	SoundMAX	5.10.01.4160	
Realtek Semiconductor Corp.	Realtek High Definition Audio Driver	1.92	
Microsoft Corporation	MSXML 4.0 SP2 (KB973688)	4.20.9876.0	
Microsoft Corporation	Microsoft .NET Framework 4 Client Profile PTG Language Pack	4.0.30319	
ATI	CCC Help Norwegian	2009.0303.2223.40202	
Microsoft Corporation	Microsoft Windows XP Professional	5.1.2600	Service Pack 3

Figura 44 – OCS-Inventory, inventário de *software*

O "OCS-Inventory" mostrou-se uma aplicação imprescindível na Câmara pois com ela, neste momento, pode-se obter relatórios detalhados das máquinas que se encontram obsoletas e precisam de atualizações, quer de *hardware* e/ou *software*, quantificar os computadores que possuem determinado *software*, descobrir quem utiliza determinado computador, etc.

6. Conclusões e trabalho futuro

Este capítulo apresenta a síntese do trabalho desenvolvido e apresentado nesta tese. São também apresentados os objetivos alcançados, as limitações e perspetivas de desenvolvimento futuro.

6.1.Resumo

Sendo a Câmara Municipal de Santo Tirso uma instituição pública cujo seu principal foco é o munícipe é importante garantir o bom funcionamento dos serviços disponibilizados. Pelo que é fundamental que todos esses serviços funcionem de uma forma fluida e se possível sem contratempos para que os cidadãos do município se sintam satisfeitos com os serviços prestados.

Na atualidade, a influência da informática nos restantes serviços municipalizados é vista como um fator de produtividade porque a sua principal função é disponibilizar e manter as ferramentas/aplicações utilizadas no dia-a-dia pelos colaboradores.

Ao longo dos anos, o serviço de informática da Câmara Municipal de Santo Tirso tentou acompanhar a rápida evolução e dependência tecnológica dos serviços prestados pelos seus colaboradores.
O Serviço de informática nasceu com a necessidade de uma aplicação de contabilidade e faturação, sendo que no início havia um único computador na Câmara.
Atualmente, praticamente todos os colaboradores têm à sua disposição um posto de trabalho com um computador e com acesso a conteúdos nos servidores e na internet.
Para conseguir esta dimensão foi necessário adquirir equipamentos de rede, servidores, contruir boas infraestruturas para passagem de cabos etc.

Durante este percurso foi-se sentido a necessidade de monitorizar os equipamentos de rede e os serviços disponibilizados nos servidores para que em caso de anomalias os seus administradores fossem notificados com vista a proceder à sua reparação e resolução.

Para colmatar esta necessidade de monitorização decidiu-se realizar um estudo no âmbito desta temática para encontrar a ferramenta mais adequada à rede de comunicações de dados da Câmara Municipal de Santo Tirso.
Após a realização desse estudo concluiu-se que o “Nagios” é a aplicação de monitorização que preenchia os requisitos necessários para alcançar os objetivos propostos.

No decorrer deste estudo foram ainda encontradas outras de ferramentas complementares à monitorização, a ser feita pelo Nagios, e que revelaram também muito úteis, tais como *o "*NTOPNG*"* e o "OCS-Inventory*"*.

6.2.Objetivos Alcançados

O primeiro objetivo deste trabalho foi efetuar um estudo aprofundado da área de gestão de redes. Foram estudados conceitos e noções fundamentais, desde a importância que a gestão de redes assume em qualquer ambiente informático, passando pelas áreas funcionais existentes, até ao Modelo arquitetural, Modelo de informação de gestão e Modelo relacional de gestão.

Seguiu-se uma análise aprofundada sobre a rede da Câmara com vista a ser feita um levantamento dos requisitos necessários para geria a rede.

Pretendia-se compreender quais as necessidades existentes e que seriam determinantes para a configuração das aplicações escolhidas para efetuar a gestão da rede.

Seguiu-se a implementação da aplicação "Nagios" de acordo com as configurações estabelecidas. A tarefa de monitorização revelou-se determinante uma vez que permitiu detetar anomalias nas comunicações e simultaneamente fornecer informação aos gestores da rede para que estes, com rapidez, atuassem no sentido da resolução desses problemas.
As ferramentas de monitorização e de inventário revelaram-se de elevada utilidade permitindo conhecer melhor a infraestrutura. A informação adquirida com as diferentes aplicações implementadas, "NOTOPNG", "OCS-Inventory", "MRTG" permitiu caracterizar a rede relativamente a equipamento e serviços disponíveis, contribuindo para um melhor funcionamento dos serviços de informática na Câmara Municipal de Santo Tirso.

.

6.3.Limitações e Trabalho Futuro

A rede da Câmara começou pequena mas ao longo dos anos foi crescendo substancialmente, quer em número de equipamentos, quer no número de serviços disponibilizados por estes. Nunca foi pensado segmentar a rede sendo constituída por uma única rede onde se incluem todos os equipamentos ligados, não fazendo a separação por tipo de equipamentos.

Este estudo permitiu também compreender a necessidade em segmentar a rede num futuro próximo. Para tal, seria necessária criar as seguintes *vlan's*:

- *Vlan* para servidores;
- *Vlan* para impressoras;
- *Vlan* para computadores de funcionários;
- *Vlan* de gestão dos equipamentos ativos de rede;
- *Vlan* para os administradores de rede.

A segmentação da rede tem as seguintes vantagens:

- A segmentação de rede através de *vlan's* melhora a monitorização que pode ser feita em cada uma delas pelo sistema de monitorização. Diminui o ruído e tráfego porque este será dividido pelas *Vlan's*;
- A gestão e monitorização de equipamentos ativos de rede e servidores seria muito mais eficaz;
- A análise de protocolos, por parte do "NTOPNG", seria mais organizada pois permitia diferenciar o tráfego por *vlan*;
- Permitia tirar mais partido das potencialidades dos *switches*. Pois é possível fazer controlo de tráfego em L2 (Data-Link), mais eficaz do que em L7 (aplicacional -TMG).

Depois de organizar e desenhar a rede é possível tirar partido de todas as funcionalidades das aplicações aqui estudadas assim como passar a existir um melhor desempenho das aplicações de rede utilizados pelos colaboradores.

Com a aplicação "NTOPNG" foi constato que na rede existe muito ruído de *broadcast* principalmente gerado pelas impressoras. Este ruído podia ser eliminado com a utilização de uma *vlan* para impressoras.

1. Trabalho futuro – "Nagios"

A Câmara Municipal de Santo Tirso possui outro tipo de equipamento espalhado pelo município e que seria interessante incluir na monitorização da rede. Nomeadamente, torniquetes nas piscinas municipais, camaras de vídeo vigilância em rede e da contagem de folhas impressas por utilizador.

2. Trabalho futuro – "NTOPNG"

Com o "NTOPNG" pretende-se classificar e monitorizar melhor os protocolos de rede que circulam na rede. A segmentação de rede vem facilitar bastante este objetivo.

Bibliografia

Alexander Clemm, P. (2006). *Network Management Fundamentals.* Indianapolis, IN 46240 USA: Cisco Press.

Castelli. (2002). *Network Management Architecture*. Obtido de http://flylib.com/books/en/2.59.1.162/1/

Cisco. (2012). *Chapter 10 SNMP and the Management Information Base.*

Ed Tittel. (2012). *Unified Threat Management For Dummies.* John Wiley & Sons, Inc.

Francisco Fonseca, C. d. (2012). Obtido de http://www.semanainformatica.xl.pt/gestao/gestao/solucoes-de-monitorizacao-ganham-importancia

Icinga. (2014). *Icinga*. Obtido de Icinga: https://www.icinga.org/icinga/screenshots/icinga-classic/

José Ferraz, s. s. (2012). *semanainformatica*. Obtido de http://www.semanainformatica.xl.pt/gestao/gestao/solucoes-de-monitorizacao-ganham-importancia

mrtg. (2015). *mrtg*. Obtido de mrtg: http://www.menalto.com/gallery/d/42433-2/mrtg-pronto.png

Nagios_vs_Icinga. (08 de 2011). *Nagios vs Icinga*. Obtido de Nagios vs Icinga: http://assets.nagios.com/datasheets/compare/How_Nagios_Compares_To_Icinga.pdf

NagiosMap. (2006). Obtido de http://imagegator.net/base-images-nagios/0.

NNMI. (2015). Obtido de http://www8.hp.com/us/en/software-solutions/network-node-manager-i-network-management-software/.

NTOPNG. (2015). Obtido de http://www.ntop.org/wp-content/uploads/2013/06/ActiveFlows.png?w=515

NTOPNG. (2015). Obtido de http://www.ntop.org/products/ntop/

OCS Iventory. (2014). *OCS Inventory*. Obtido de OCS Inventory: http://www.ocsinventory-ng.org/en/screenshots.html

OCS Windows Agent. (2013). *ocsinventory*. Obtido de ocsinventory: http://wiki.ocsinventory-ng.org/index.php/Documentation:WindowsAgent

Opsview. (2015). *Opsview*. Obtido de Opsview: http://www.opsview.com/why-opsview/easy-setup

Opsview Development Team. (28 de 11 de 2011). *techworld*. Obtido de techworld: http://www.techworld.com/blogs/monitoring-the-pulse-of-it/gaining-an-edge-with-opsview-open-source-monitoring-3538048/

Oreilly. (2009). Obtido de http://archive.oreilly.com/pub/a/perl/excerpts/system-admin-with-perl/twenty-minute-snmp-tutorial.html.

PNP4Nagios. (2010). *PNP4Nagios*. Obtido de PNP4Nagios: http://blog.nicolargo.com/wp-content/uploads/2010/09/S%C3%A9lection_048.png

PNP4nagios. (2013). *PNP4nagios*. Obtido de PNP4nagios: https://docs.pnp4nagios.org/pnp-0.6/start

Qi, H. (2001). Obtido de http://maf.sourceforge.net/

Scbmidt, D. R. (2005). *Essential SNMP 2nd Edition.* O'Reilly Media.

Schmidt, D. R. (2005). *Essential SNMP.* O'Reilly Media.

SérgioSá. (2012). Obtido de http://www.semanainformatica.xl.pt/gestao/gestao/solucoes-de-monitorizacao-ganham-importancia

Tony Bautts, T. D. (2005). *Linux Network Administrator's Guide - Third Edition.* O'Reilly Media Inc.